



IPアドレッシング : IPv4 アドレッシングコンフィギュレーションガイド

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 : シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間 : 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

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

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

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

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.



目次

最初にお読みください 1

IPv4 アドレスの設定 3

機能情報の確認 3

IP アドレスに関する情報 4

2 進数ナンバリング 4

IP アドレスの構造 6

IP アドレス クラス 7

IP ネットワークのサブネット化 9

IP ネットワーク アドレス割り当て 11

Classless Inter-Domain Routing 14

Prefixes 14

IP アドレスの設定方法 15

IP アドレスをインターフェイスに割り当てることに起因する、ネットワークとの IP 接続の確立 15

トラブルシューティングのヒント 16

セカンダリ IP アドレスの使用によるネットワークでサポートされる IP ホストの数の増加 16

トラブルシューティングのヒント 18

次の作業 18

IP サブネットゼロの使用を許可することによる、使用可能な IP サブネット数の最大化 18

トラブルシューティングのヒント 19

ネットワーク マスク形式の指定 20

現在のセッションにおけるネットマスク表示形式の指定 20

個々の回線におけるネットマスク表示形式の指定 20

ポイントツーポイント WAN インターフェイスの IP アンナumberド インターフェイスを使用することによる必要な IP アドレスの数の制限 22

IP アンナナバード機能	22
トラブルシューティングのヒント	24
ポイントツーポイント WAN インターフェイスの 31 ビットプレフィックスの IP アドレスを使用することによる必要な IP アドレスの数の制限	24
RFC 3021	24
トラブルシューティングのヒント	27
IP アドレスの設定例	28
例：IP アドレスをインターフェイスに割り当てることに起因する、ネットワークとの IP 接続の確立	28
例：セカンダリ IP アドレスの使用によるネットワークでサポートされる IP ホストの数の増加	28
例：ポイントツーポイント WAN インターフェイスの IP アンナナバードインターフェイスを使用することによる必要な IP アドレスの数の制限	29
例：ポイントツーポイント WAN インターフェイスの 31 ビットプレフィックスの IP アドレスを使用することによる必要な IP アドレスの数の制限	29
例：IP サブネットゼロの使用を許可することによる、使用可能な IP サブネット数の最大化	29
次の作業	30
その他の参考資料	30
IP アドレスの機能情報	31
IP オーバーラッピング アドレス プール	35
機能情報の確認	35
IP オーバーラッピング アドレス プールの制約事項	36
自動 IP オーバーラッピング アドレス プールに関する情報	36
利点	36
IP アドレス グループの仕組み	36
IP オーバーラッピング アドレス プールの設定方法	37
ローカル プール グループの設定および確認	37
IP オーバーラッピング アドレス プールの設定の設定例	38
グローバルデフォルトメカニズムとしてのローカルアドレスプーリングの定義例	38
複数範囲の IP アドレスの単一プールへの設定例	38
その他の参考資料	38

IP オーバーラッピング アドレス プールの設定の機能情報	40
用語集	41
自動 IP アンナバード イーサネット ポーリングのサポート	43
機能情報の確認	43
IP アンナバード イーサネット ポーリングのサポートに関する情報	44
自動 IP アンナバード イーサネット ポーリング サポートの概要	44
IP アンナバード イーサネット ポーリングのサポートの設定方法	44
イーサネット インターフェイスのポーリングのイネーブル化	44
アンナバード インターフェイスの IP ARP ポーリング用のキューのサイズとパケット レートの設定	46
IP アンナバード イーサネット ポーリング サポートの確認	47
IP アンナバード イーサネット ポーリングのサポートの設定例	48
例：イーサネット インターフェイスのポーリングのイネーブル化	48
例：アンナバード インターフェイスの IP ARP ポーリング用のキューのサイズとパケット レートの設定	48
その他の参考資料	49
IP アンナバード イーサネット ポーリングのサポートの機能情報	49
自動 IP	51
機能情報の確認	52
自動 IP の前提条件	52
自動 IP の制約事項	52
自動 IP に関する情報	53
自動 IP の概要	53
Seed Device	56
自動 IP リングにデバイスを挿入するための自動 IP 設定	57
自動 IP リングからのデバイスの削除	59
自動スワップ テクニックを使用した競合解決	60
自動 IP の設定方法	62
シード デバイスの設定	62
ノード インターフェイス上における自動 IP 機能の設定（自動 IP リングへの組み込み用）	64
自動 IP の確認とトラブルシューティング	67

自動 IP の設定例	69
例：シード デバイスの設定	69
例：ノード インターフェイス上における自動 IP 機能の設定（自動 IP リングへの組み込み用）	69
自動 IP に関する追加情報	69
自動 IP の機能情報	70
ゼロ タッチ自動 IP	71
機能情報の確認	71
ゼロ タッチ自動 IP の前提条件	72
ゼロ タッチ自動 IP の制約事項	72
ゼロ タッチ自動 IP に関する情報	72
ゼロ タッチ自動 IP の設定方法	75
自動 IP サーバと自律型ネットワークの関連付け	75
自動 IP リング ポート上での auto モードのイネーブル化	77
自動 IP サーバの設定とサーバ上での IP アドレス プールの予約	79
シード ポートの設定	80
ゼロ タッチ自動 IP の確認とトラブルシューティング	81
ゼロ タッチ自動 IP の設定例	84
例：自動 IP サーバと自律型ネットワークの関連付け	84
例：自動 IP リング ポート上での auto モードのイネーブル化	84
例：自動 IP サーバの設定とサーバ上での IP アドレス プールの予約	84
例：シード ポートの設定	85
ゼロ タッチ自動 IP に関する追加情報	85
自動 IP の機能情報	86



第 1 章

最初にお読みください

Cisco IOS XE 16 についての重要事項

Cisco IOS XE Release 3.7.0E (Catalyst スイッチ) と Cisco IOS XE Release 3.17S (アクセスおよびエッジルーティング) という有効な 2 つのリリースが統合され、スイッチングおよびルーティング ポートフォリオ内のアクセスおよびエッジ製品を幅広く網羅する 1 つの統合リリースバージョン (Cisco IOS XE 16) へと進化しました。



(注) 機能が導入されると、技術構成ガイドの [Feature Information] テーブルで通知されます。その機能に対応している他のプラットフォームについては、通知される場合と通知されない場合があります。特定の機能がプラットフォームでサポートされているかどうかを確認するには、製品のランディングページに表示される技術構成ガイドをご覧ください。製品のランディングページに技術構成ガイドが表示された場合、そのプラットフォームでは機能がサポートされています。



第 2 章

IPv4 アドレスの設定

この章では、ネットワーキングデバイスの一部であるインターフェイスでの IPv4 アドレスの設定およびその手順について説明します。



(注) このマニュアルでは、これ以降 IPv4 アドレスを示す場合、IPv4 ではなく、IP だけ使用します。

- [機能情報の確認, 3 ページ](#)
- [IP アドレスに関する情報, 4 ページ](#)
- [IP アドレスの設定方法, 15 ページ](#)
- [IP アドレスの設定例, 28 ページ](#)
- [次の作業, 30 ページ](#)
- [その他の参考資料, 30 ページ](#)
- [IP アドレスの機能情報, 31 ページ](#)

機能情報の確認

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

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

IP アドレスに関する情報

2 進数ナンバリング

IP アドレスは 32 ビット長です。32 ビットは 4 つのオクテット (8 ビット) に分割されます。2 進数ナンバリングの基本を理解しておく、ネットワークで IP アドレスを管理する場合に非常に役に立ちます。これは、32 ビットの値が変わると、別の IP ネットワークアドレスまたは IP ホストアドレスのいずれかを示すためです。

2 進数の値は、右から左に順番に 0 ~ 7 で累乗した 2 を、各位置の数 (0 または 1) に掛けた数値で表されます。以下の図は、8 桁の 2 進数の例を示します。

図 1: 8 桁の 2 進数の例

128	64	32	16	8	4	2	1
$1 \cdot 2^7$	$1 \cdot 2^6$	$1 \cdot 2^5$	$1 \cdot 2^4$	$1 \cdot 2^3$	$1 \cdot 2^2$	$1 \cdot 2^1$	$1 \cdot 2^0$
1	1	1	1	1	1	1	1

128
64
32
16
8
4
2
1
+
<hr/>
= 255

180206

以下の図は、0～134における2進数から10進数への変換例を示します。

図2: 0～134における2進数から10進数への変換

00000000 = 000	00011011 = 027	00110110 = 054	01010001 = 081	01101100 = 108
00000001 = 001	00011100 = 028	00110111 = 055	01010010 = 082	01101101 = 109
00000010 = 002	00011101 = 029	00111000 = 056	01010011 = 083	01101110 = 110
00000011 = 003	00011110 = 030	00111001 = 057	01010100 = 084	01101111 = 111
00000100 = 004	00011111 = 031	00111010 = 058	01010101 = 085	01110000 = 112
00000101 = 005	00100000 = 032	00111011 = 059	01010110 = 086	01110001 = 113
00000110 = 006	00100001 = 033	00111100 = 060	01010111 = 087	01110010 = 114
00000111 = 007	00100010 = 034	00111101 = 061	01011000 = 088	01110011 = 115
00001000 = 008	00100011 = 035	00111110 = 062	01011001 = 089	01110100 = 116
00001001 = 009	00100100 = 036	00111111 = 063	01011010 = 090	01110101 = 117
00001010 = 010	00100101 = 037	01000000 = 064	01011011 = 091	01110110 = 118
00001011 = 011	00100110 = 038	01000001 = 065	01011100 = 092	01110111 = 119
00001100 = 012	00100111 = 039	01000010 = 066	01011101 = 093	01111000 = 120
00001101 = 013	00101000 = 040	01000011 = 067	01011110 = 094	01111001 = 121
00001110 = 014	00101001 = 041	01000100 = 068	01011111 = 095	01111010 = 122
00001111 = 015	00101010 = 042	01000101 = 069	01100000 = 096	01111011 = 123
00010000 = 016	00101011 = 043	01000110 = 070	01100001 = 097	01111100 = 124
00010001 = 017	00101100 = 044	01000111 = 071	01100010 = 098	01111101 = 125
00010010 = 018	00101101 = 045	01001000 = 072	01100011 = 099	01111110 = 126
00010011 = 019	00101110 = 046	01001001 = 073	01100100 = 100	01111111 = 127
00010100 = 020	00101111 = 047	01001010 = 074	01100101 = 101	10000000 = 128
00010101 = 021	00110000 = 048	01001011 = 075	01100110 = 102	10000001 = 129
00010110 = 022	00110001 = 049	01001100 = 076	01100111 = 103	10000010 = 130
00010111 = 023	00110010 = 050	01001101 = 077	01101000 = 104	10000011 = 131
00011000 = 024	00110011 = 051	01001110 = 078	01101001 = 105	10000100 = 132
00011001 = 025	00110100 = 052	01001111 = 079	01101010 = 106	10000101 = 133
00011010 = 026	00110101 = 053	01010000 = 080	01101011 = 107	10000110 = 134

以下の図は、135 ~ 255 における 2 進数から 10 進数の変換例を示します。

図 3: 135 ~ 255 における 2 進数から 10 進数への変換

10000111 = 135	10100010 = 162	10111101 = 189	11011000 = 216	11110011 = 243
10001000 = 136	10100011 = 163	10111110 = 190	11011001 = 217	11110100 = 244
10001001 = 137	10100100 = 164	10111111 = 191	11011010 = 218	11110101 = 245
10001010 = 138	10100101 = 165	11000000 = 192	11011011 = 219	11110110 = 246
10001011 = 139	10100110 = 166	11000001 = 193	11011100 = 220	11110111 = 247
10001100 = 140	10100111 = 167	11000010 = 194	11011101 = 221	11111000 = 248
10001101 = 141	10101000 = 168	11000011 = 195	11011110 = 222	11111001 = 249
10001110 = 142	10101001 = 169	11000100 = 196	11011111 = 223	11111010 = 250
10001111 = 143	10101010 = 170	11000101 = 197	11100000 = 224	11111011 = 251
10010000 = 144	10101011 = 171	11000110 = 198	11100001 = 225	11111100 = 252
10010001 = 145	10101100 = 172	11000111 = 199	11100010 = 226	11111101 = 253
10010010 = 146	10101101 = 173	11001000 = 200	11100011 = 227	11111110 = 254
10010011 = 147	10101110 = 174	11001001 = 201	11100100 = 228	11111111 = 255
10010100 = 148	10101111 = 175	11001010 = 202	11100101 = 229	
10010101 = 149	10110000 = 176	11001011 = 203	11100110 = 230	
10010110 = 150	10110001 = 177	11001100 = 204	11100111 = 231	
10010111 = 151	10110010 = 178	11001101 = 205	11101000 = 232	
10011000 = 152	10110011 = 179	11001110 = 206	11101001 = 233	
10011001 = 153	10110100 = 180	11001111 = 207	11101010 = 234	
10011010 = 154	10110101 = 181	11010000 = 208	11101011 = 235	
10011011 = 155	10110110 = 182	11010001 = 209	11101100 = 236	
10011100 = 156	10110111 = 183	11010010 = 210	11101101 = 237	
10011101 = 157	10111000 = 184	11010011 = 211	11101110 = 238	
10011110 = 158	10111001 = 185	11010100 = 212	11101111 = 239	
10011111 = 159	10111010 = 186	11010101 = 213	11110000 = 240	
10100000 = 160	10111011 = 187	11010110 = 214	11110001 = 241	
10100001 = 161	10111100 = 188	11010111 = 215	11110010 = 242	

IP アドレスの構造

IP ホスト アドレスは、IP パケットを送信できるデバイスを示します。IP ネットワーク アドレスは、1 つ以上のホストが接続できる特定のネットワーク セグメントを示します。次に、IP アドレスの特性を示します。

- IP アドレスは 32 ビット長です。
- IP アドレスは、それぞれが 1 バイト（オクテット）の 4 セクションに分割されます。
- IP アドレスは、通常、ドット付き 10 進で知られる形式で記述されます。

以下の表に、IP アドレスの例をいくつか示します。

表 1: IP アドレスの例

ドット付き 10 進形式の IP アドレス	2 進数形式の IP アドレス
10.34.216.75	00001010.00100010.11011000.01001011
172.16.89.34	10101100.00010000.01011001.00100010

ドット付き 10 進形式の IP アドレス	2 進数形式の IP アドレス
192.168.100.4	11000000.10101000.01100100.00000100



(注) 上記の表内の IP アドレスは、RFC 1918 『Address Allocation for Private Internets』 のものです。これらの IP アドレスは、インターネット上でルーティングできません。これらは、プライベートネットワークで使用されます。RFC1918 の詳細については、<http://www.ietf.org/rfc/rfc1918.txt> を参照してください。

IP アドレスは、ネットワークおよびホストとして知られる 2 つのセクションにさらに分割されます。この分割は、IP アドレスからクラスの任意の範囲で行われます。詳細については、RFC 791 『Internet Protocol』 (<http://www.ietf.org/rfc/rfc0791.txt>) を参照してください。

IP アドレス クラス

IP アドレスの割り当て方法にいくつかの構造を提供するため、IP アドレスはクラスにグループ化されます。各クラスには、IP アドレスの範囲があります。各クラスの IP アドレスの範囲は、32 ビット IP アドレスのネットワーク セクションに割り当てられるビットの数により決まります。ネットワーク セクションに割り当てられるビットの数は、ドット付き 10 進形式のマスク、または略字 /*n* (ここで *n* はマスクのビットの数です) で表されます。

以下の表に、クラスおよび各クラスに関連付けられるマスクごとの IP アドレスの範囲のリストを示します。太字の数値は、各クラスの IP アドレスのネットワーク セクションを示します。他の数値は、ホスト IP アドレスに使用できます。たとえば、IP アドレス 10.90.45.1、マスク 255.0.0.0 は、ネットワーク IP アドレス 10.0.0.0 およびホスト IP アドレス 0.90.45.1 に分割されます。

表 2: クラスおよびマスク別の IP アドレス範囲

クラス	範囲
A (ドット付き 10 進形式の範囲/マスク)	0.0.0.0 ~ 127.0.0.0/8 (255.0.0.0)
A (2 進数形式の範囲)	00000000.00000000.00000000.00000000 ~ 01111111.00000000.00000000.00000000
A (2 進数形式のマスク)	11111111.00000000.00000000.00000000/8
B (ドット付き 10 進形式の範囲/マスク)	128.0.0.0 ~ 191.255.0.0 /16 (255.255.0.0)
B (2 進数形式の範囲)	10000000.00000000.00000000.00000000 ~ 10111111.11111111.00000000.00000000
B (2 進数形式のマスク)	11111111.11111111.00000000.00000000 /16

クラス	範囲
C (ドット付き 10 進形式の範囲/マスク)	192.0.0.0 ~ 223.255.255.0/24 (255.255.255.0)
C (2 進数形式の範囲)	11000000.00000000.00000000.00000000 ~ 11011111.11111111.11111111.00000000
C (2 進数形式のマスク)	11111111.11111111.11111111.00000000/24
D ¹ (ドット付き 10 進形式の範囲/マスク)	224.0.0.0 ~ 239.255.255.255/32 (255.255.255.255)
D (2 進数形式の範囲)	11100000.00000000.00000000.00000000 ~ 11101111.11111111.11111111.11111111
D (2 進数形式のマスク)	11111111.11111111.11111111.11111111/32
E ² (ドット付き 10 進形式の範囲/マスク)	240.0.0.0 ~ 255.255.255.255/32 (255.255.255.255)
E (2 進数形式の範囲)	11110000.00000000.00000000.00000000 ~ 11111111.11111111.11111111.11111111
E (2 進数形式のマスク)	11111111.11111111.11111111.11111111/32

¹ クラス D の IP アドレスは、マルチキャストアプリケーション用に予約されています。

² クラス E の IP アドレスは、ブロードキャストトラフィック用に予約されています。



(注) これらの範囲の一部の IP アドレスは、特殊な目的のために予約されています。詳細については、RFC 3330 『Special-Use IP Addresses』 (<http://www.ietf.org/rfc/rfc3330.txt>) を参照してください。

ネットワーク マスク内の数値が 1 から 0 または 0 から 1 に変更されると、ネットワーク アドレスが変わります。たとえば、10101100.00010000.01011001.00100010/16 を 10101100.00110000.01011001.00100010/16 に変更すると、ネットワーク アドレスが 172.16.89.34/16 から 172.48.89.34/16 に変わります。

ネットワーク マスク外の数値が 1 から 0 または 0 から 1 に変更されると、ホストアドレスが変わります。たとえば、10101100.00010000.01011001.00100010/16 を 10101100.00010000.01011001.00100011/16 に変更すると、ホストアドレスが 172.16.89.34/16 から 172.16.89.35/16 に変わります。

各クラスの IP アドレスは、特定の範囲の IP ネットワークアドレスおよび IP ホストアドレスをサポートします。各クラスで使用可能な IP ネットワークアドレスの範囲は、使用可能なビットの数で 2 を累乗した式で求められます。クラス A アドレスの場合、最初のオクテット（上記の表を参

照)の最初のビットの値は常に0です。7ビットは、追加ネットワークアドレスの作成用です。そのため、クラスAで使用可能なIPネットワークアドレスは128あります(2の7乗=128)。

IPアドレスクラスで使用可能なIPホストアドレスの数は、使用可能なビットの数で2を累乗し2を引いた数で求められます。IPホストアドレスのクラスAアドレスで使用可能なビットは24あります。そのため、クラスAで使用可能なIPホストアドレスは16,777,214あります((2の24乗)-2=16,777,214)。



(注) 累乗した数から2を引くのは、ホストで使用できないIPアドレスが2つあるためです。すべて0のホストアドレスは、ネットワークアドレスと同じになるため使用できません。たとえば、10.0.0.0は、IPネットワークアドレスとIPホストアドレスの両方で使用できません。すべて1のアドレスは、ネットワークのすべてのホストにアクセスするときに使用されるブロードキャストアドレスです。たとえば、アドレスが10.255.255.255のIPデータグラムは、ネットワーク10.0.0.0のすべてのホストにより受け入れられます。

以下の表に、各クラスのIPアドレスで使用可能なネットワークおよびホストアドレスを示します。

表3: 各クラスのIPアドレスで使用可能なネットワークおよびホストアドレス

クラス	ネットワークアドレス	ホストアドレス
A	128	16,777,214
B	16,384 ³	65,534
C	2,097,152 ⁴	254

³ 表2に示すように、最初の2ビットは常に10になるため、クラスBのIPネットワークアドレスで使用可能なのは14ビットだけです。

⁴ 表3に示すように、最初の2ビットは常に110になるため、クラスCのIPネットワークアドレスで使用可能なのは21ビットだけです。

IP ネットワークのサブネット化

IPアドレスクラスのネットワークおよびホストビットを任意に分割したことで、IPスペースの割り当てが非効率的になりました。たとえば、ネットワークに16の物理セグメントがある場合、16のIPネットワークアドレスが必要です。16のクラスBのIPネットワークアドレスを使用する場合、各物理セグメントで65,534のホストをサポートできます。サポートされるホストIPアドレスは合計で1,048,544(16 * 65,534 = 1,048,544)です。単一のネットワークセグメントで65,534のホストを使用可能なネットワークテクノロジーはあまりありません。また、1,048,544のIPホストアドレスを必要とする組織もあまりありません。この問題では、同様のIPサブネットワークアドレスのグループにIPネットワークアドレスを分割できる新しい戦略を開発する必要があります。この戦略は、サブネット化と呼ばれます。

たとえば、ネットワークに16の物理セグメントがある場合、16のIPサブネットワークアドレスが必要です。これは、1つのクラスBのIPアドレスで実現できます。たとえば、クラスBのIP

アドレス 172.16.0.0 の場合、3 番目のオクテットから 4 ビットをサブネット ビットとして予約できます。これにより、16 個のサブネット IP アドレスを使用できます (2 の 4 乗 = 16)。次の表に、172.16.0.0/20 の IP サブネットを示します。

表 4: 172.16.0.0/20 を使用した IP サブネットアドレスの例

番号	ドット付き 10 進形式の IP サブネットアドレス	2 進数形式の IP サブネットアドレス
0 ⁵	172.16.0.0	10101100.00010000.00000000.00000000
1	172.16.16.0	10101100.00010000.00010000.00000000
2	172.16.32.0	10101100.00010000.00100000.00000000
3	172.16.48.0	10101100.00010000.00110000.00000000
4	172.16.64.0	10101100.00010000.01000000.00000000
5	172.16.80.0	10101100.00010000.01010000.00000000
6	172.16.96.0	10101100.00010000.01100000.00000000
7	172.16.112.0	10101100.00010000.01110000.00000000
8	172.16.128.0	10101100.00010000.10000000.00000000
9	172.16.144.0	10101100.00010000.10010000.00000000
10	172.16.160.0	10101100.00010000.10100000.00000000
11	172.16.176.0	10101100.00010000.10110000.00000000
12	172.16.192.0	10101100.00010000.11000000.00000000
13	172.16.208.0	10101100.00010000.11010000.00000000
14	172.16.224.0	10101100.00010000.11100000.00000000
15	172.16.240.0	10101100.00010000.11110000.00000000

⁵ サブネット ビットがすべて 0 に設定されている最初のサブネットは、サブネット 0 と呼ばれます。これはネットワーク アドレスとの区別ができないため、注意して使用する必要があります。

サブネットワーク (サブネット) マスク内の数値が 1 から 0 または 0 から 1 に変更されると、サブネットワーク アドレスが変わります。たとえば、10101100.00010000.01011001.00100010/20 を 10101100.00010000.01111001.00100010/20 に変更すると、ネットワーク アドレスが 172.16.89.34/20 から 172.16.121.34/20 に変わります。

サブネット マスク内の数値が 1 から 0 または 0 から 1 に変更されると、ホスト アドレスが変わります。たとえば、10101100.00010000.01011001.00100010/20 から 10101100.00010000.01011001.00100011/20 に変更すると、ホスト アドレスが 172.16.89.34/20 から 172.16.89.35/20 に変わります。



ワンポイントアドバイス

手動による IP ネットワーク、サブネットワークおよびホストの計算の必要性をなくすには、インターネットで利用できるいずれかの無料の IP サブネット カリキュレータを使用します。

ネットワークアドレスとサブネットまたはサブネットワークアドレスという用語は混同しやすいこともあります。また、これらを使用する状況も複雑な場合があります。一般的に、ネットワークアドレスという用語は、「特定のネットワーク セグメント用の宛先 IP ホストでトラフィックを受信できるように、ルータがトラフィックをそのセグメントに送信するときに使用する IP アドレス」を表します。そのため、ネットワークアドレスという用語は、サブネット化されていない IP ネットワークアドレスとサブネット化された IP ネットワークアドレスの両方に使用できます。実際はサブネット化されたネットワークアドレスである特定の IP ネットワークアドレスにルータからトラフィックを転送するときの問題をトラブルシューティングする場合、宛先ネットワークアドレスをサブネットネットワークアドレスとするとより詳しくなります。これは、ルーティングプロトコルによっては、サブネット ネットワーク ルートとネットワーク ルートのアドバタイズの処理が異なる場合があるためです。たとえば、RIP v2 のデフォルトの動作では、ルーティングアップデートを他のルータに送信するときに、サブネット化されていないネットワークアドレス (172.16.32.0/24 は RIP v2 により 172.16.0.0/16 としてアドバタイズされます) に接続されるようにサブネットネットワークアドレスを自動的に集約します。そのため、他のルータが、ネットワークの IP ネットワーク アドレスを認識している場合もありますが、その IP ネットワークアドレスのサブネット化されたネットワーク アドレスを認識していない場合もあります。



ヒント

IP アドレス空間という用語は、IP アドレスの範囲を示すときに使用されることがあります。次に例を示します。「現在の IP アドレス空間で使用可能なすべての IP アドレスを使用しているために新しい IP ネットワーク アドレスをネットワークに割り当てる必要があります。」

IP ネットワーク アドレス割り当て

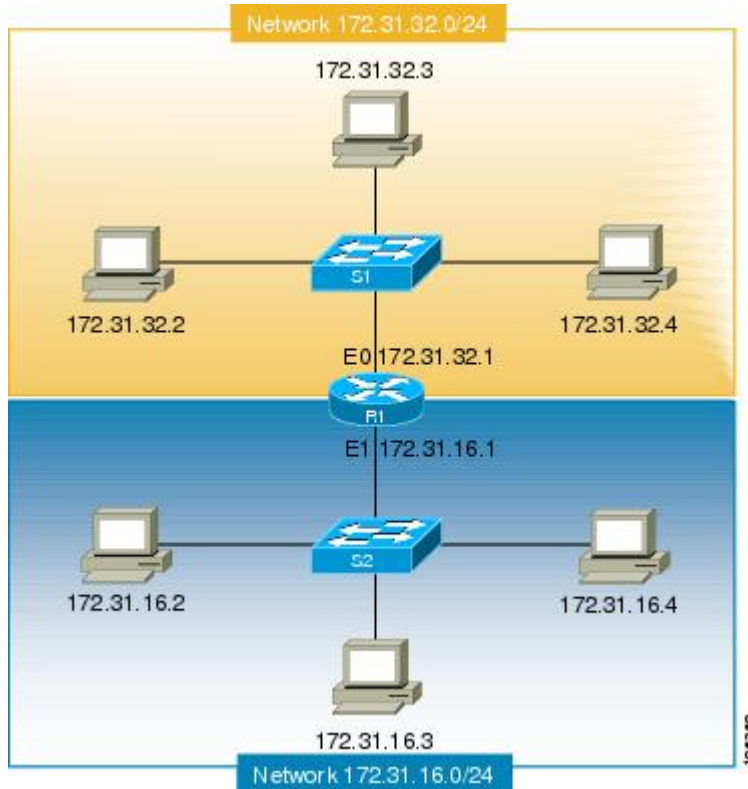
ルータは、IP ネットワーク アドレスを追跡し、ネットワークのネットワーク IP トポロジ (OSI リファレンス モデルのレイヤ 3) を理解して、IP トラフィックを正しくルートできます。ルータがネットワーク層 (IP) トポロジを理解できるようにするには、ルータにより他の物理ネットワークセグメントから分離されているすべての個々の物理ネットワークセグメントに、固有の IP ネットワーク アドレスが必要です。

以下の図に、IP ネットワーク アドレスが正しく設定された簡単なネットワークの例を示します。R1 内のルーティング テーブルは、次の表のようになります。

表 5: 正しく設定されたネットワークのルーティングテーブル

インターフェイス イーサネット 0	インターフェイス イーサネット 1
172.31.32.0/24 (接続)	172.31.16.0/24 (接続)

図 4: 正しく設定されたネットワーク

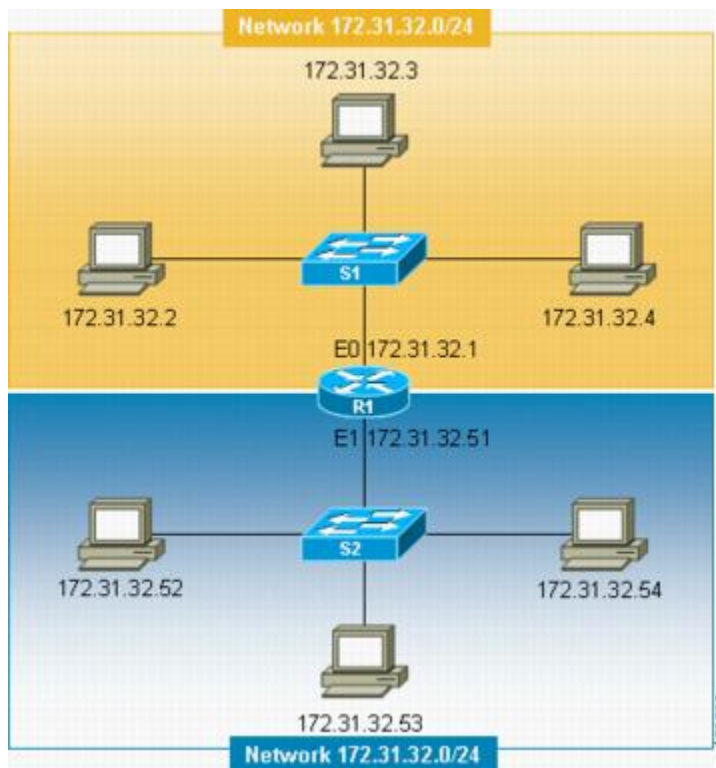


以下の図に、IP ネットワークアドレスが正しく設定されていない簡単なネットワークの例を示します。R1 内のルーティングテーブルは、次の表のようになります。IP アドレスが 172.31.32.3 の PC が、IP アドレス 172.31.32.54 の PC に IP トラフィックを送信しようとした場合、ルータ R1 は、IP アドレスが 172.31.32.54 の PC の接続先となるインターフェイスを判別できません。

表 6: 正しく設定されていないネットワークのルータ R1 のルーティングテーブル (例 1)

イーサネット 0	イーサネット 1
172.31.32.0/24 (接続)	172.31.32.0/24 (接続)

図 5: 正しく設定されていないネットワーク (例 1)



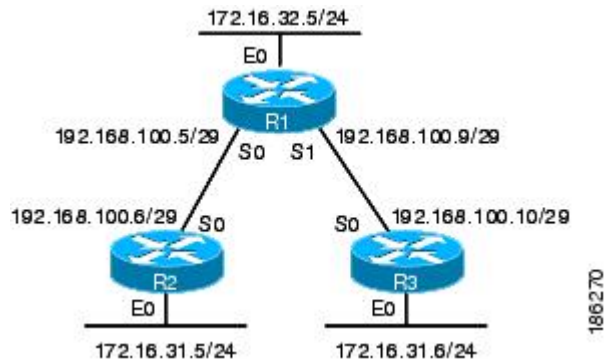
上記の図のような間違いを防止するため、Cisco IOS ベース ネットワーキング デバイスでは、IP ルーティングがイネーブルになっている場合にルータの複数のインターフェイスで同じ IP ネットワーク アドレスを設定できません。

172.16.31.0/24 が R2 および R3 で使用されている、以下の図のような間違いを防ぐ唯一の方法として、IP ネットワーク アドレスを割り当てている場所を正確に示したネットワーク ドキュメントが必要です。

表 7: 正しく設定されていないネットワークのルータ R1 のルーティング テーブル (例 2)

イーサネット 0	シリアル 0	シリアル 1
172.16.32.0/24 (接続)	192.168.100.4/29 (接続済み) 172.16.31.0/24 RIP	192.168.100.8/29 (接続済み) 172.16.31.0/24 RIP

図 6: 正しく設定されていないネットワーク (例 2)



IPルーティングの詳細については、「関連資料」セクションでIPルーティングに関連するドキュメントのリストを参照してください。

Classless Inter-Domain Routing

インターネットの使用が増加を続け、上記の表に示すように、クラス構造を使用したIPアドレスの割り当て方法には制限があるため、IPアドレスを割り当てるためのさらに柔軟な方法が必要になりました。この新しい方法については、RFC 1519『*Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*』に記載されています。CIDRにより、ネットワーク管理者は、任意のマスクをIPアドレスに適用して、管理するネットワークの要件を満たすIPアドレッシング計画を作成できます。

CIDRの詳細については、RFC 1519 (<http://www.ietf.org/rfc/rfc1519.txt>) を参照してください。

Prefixes

プレフィックスという用語は、通常、ルーティングテーブルの構築に重要なIPネットワークアドレスのビット数を示すときに使用されます。クラスフル(A、B、Cネットワークアドレス境界を厳守する)IPアドレスだけを使用する場合、プレフィックスは、アドレスのクラスのマスクと同じです。たとえば、クラスフルIPアドレッシングを使用すると、192.168.10.0などのクラスCのIPネットワークアドレスは、24ビットのマスク(/24または255.255.255.0)を使用します。また、24ビットのプレフィックスを使用するということもできます。

CIDRを使用する場合、プレフィックスは、ネットワークのルーティングテーブルをどのように読み込むかに基づいて、IPネットワークアドレスに任意に割り当てられます。たとえば、192.168.10.0、192.168.11.0、192.168.12.0、192.168.13.0など、クラスCのIPアドレスのグループは、16ビットプレフィックス(192.168.0.0/16)の192.168.0.0への単一ルートとしてアドバタイズできます。これにより、ネットワークのルータで管理が必要なルート数が1/4に削減されます。

IP アドレスの設定方法

IPアドレスをインターフェイスに割り当てることに起因する、ネットワークとのIP接続の確立

インターフェイスでIPアドレスを設定するには、次の操作を実行します。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `interfacetypenumber`
4. `noshutdown`
5. `ipaddressip-addressmask`
6. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： <code>Router> enable</code>	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	<code>configureterminal</code> 例： <code>Router# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>interfacetypenumber</code> 例： <code>Router(config)# interface fastethernet 0/0</code>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>noshutdown</code> 例： <code>Router(config-if)# no shutdown</code>	インターフェイス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 5	ipaddressip-addressmask 例 : <pre>Router(config-if)# ip address 172.16.16.1 255.255.240.0</pre>	インターフェイスの IP アドレスを設定します。
ステップ 6	end 例 : <pre>Router(config-if)# end</pre>	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、IP アドレッシングのトラブルシューティングに役に立ちます。

- **showipinterface** : インターフェイスの IP パラメータを表示します。
- **showiprouteconnected** : ネットワーキングデバイスの接続先 IP ネットワークを表示します。

セカンダリ IP アドレスの使用によるネットワークでサポートされる IP ホストの数の増加

ネットワーク セグメントを割り当てているサブネットで使用可能な IP ホストアドレスをすべて使用している状態で、ネットワークセグメントにさらに多くの IP ホストを接続する必要がある場合、セカンド IP ネットワーク アドレスをネットワーク セグメントに追加することで、サブネットが異なるすべてのホストのアドレッシングを変更する必要がなくなります。

インターフェイスでセカンダリ IP アドレスを設定するには、次の作業を実行します。

手順の概要

1. **イネーブル化**
2. **configureterminal**
3. **interfacetypenumber**
4. **noshutdown**
5. **ipaddressip-addressmask**
6. **ipaddressip-addressmasksecondary**
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	<p>イネーブル化</p> <p>例 :</p> <pre>Router> enable</pre>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	<p>configureterminal</p> <p>例 :</p> <pre>Router# configure terminal</pre>	<p>グローバル コンフィギュレーション モードを開始します。</p>
ステップ 3	<p>interfacetypenumber</p> <p>例 :</p> <pre>Router(config)# interface fastethernet 0/0</pre>	<p>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。</p>
ステップ 4	<p>noshutdown</p> <p>例 :</p> <pre>Router(config-if)# no shutdown</pre>	<p>インターフェイスをイネーブルにします。</p>
ステップ 5	<p>ipaddressip-addressmask</p> <p>例 :</p> <pre>Router(config-if)# ip address 172.16.16.1 255.255.240.0</pre>	<p>インターフェイスの IP アドレスを設定します。</p>
ステップ 6	<p>ipaddressip-addressmasksecondary</p> <p>例 :</p> <pre>Router(config-if)# ip address 172.16.32.1 255.255.240.0 secondary</pre>	<p>インターフェイスでセカンダリ IP アドレスを設定します。</p>
ステップ 7	<p>end</p> <p>例 :</p> <pre>Router(config-if)# end</pre>	<p>現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p>

トラブルシューティングのヒント

次のコマンドは、IP アドレッシングのトラブルシューティングに役に立ちます。

- **showipinterface** : インターフェイスの IP パラメータを表示します。
- **showiprouteconnected** : ネットワーキングデバイスの接続先 IP ネットワークを表示します。

次の作業

ネットワークで複数のルータを使用していて、ルーティングプロトコルをすでに設定している場合、他のルータが、割り当てられている新しい IP ネットワークにアクセスできるようにします。この場合、状況によっては、新しいネットワークをアドバタイズできるように、ルータのルーティングプロトコルの設定を変更する必要があります。ルーティングプロトコルの設定については、『Cisco IOS IP Routing: Protocol-Independent Configuration Guide』を参照してください。

IP サブネットゼロの使用を許可することによる、使用可能な IP サブネット数の最大化

ネットワークアドレスをすべて使用しているときに、ネットワークでサブネット化を使用すると、サブネットゼロを設定できるようにネットワーキングデバイスを設定できます。これにより、IP アドレッシング方式のすべてのサブネットに使用可能なネットワークアドレスが1つ追加されます。上記の表に、172.16.0.0/20 の IP サブネット（サブネット 0 を含む）を示します。

ネットワーキングデバイスで IP サブネットゼロの使用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. イネーブル化
2. `configureterminal`
3. `ipsubnet-zero`
4. `interfacetypenumber`
5. `noshutdown`
6. `ipaddressip-addressmask`
7. `end`

手順の詳細

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

	コマンドまたはアクション	目的
	例： Router> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipsubnet-zero 例： Router(config)# ip subnet-zero	IP サブネットゼロの使用をイネーブルにします。
ステップ 4	interfaceypenumber 例： Router(config)# interface fastethernet 0/0	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	noshutdown 例： Router(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 6	ipaddressip-addressmask 例： Router(config-if)# ip address 172.16.0.1 255.255.240.0	インターフェイスでサブネットゼロ IP アドレスを設定します。
ステップ 7	end 例： Router(config-if)# end	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、IP アドレッシングのトラブルシューティングに役に立ちます。

- **showipinterface** : インターフェイスの IP パラメータを表示します。

- **showiprouteconnected** : ネットワーキングデバイスの接続先 IP ネットワークを表示します。

ネットワーク マスク形式の指定

デフォルトでは、**show** コマンドは、IP アドレスおよびそのネットマスクをドット付き 10 進表記で表示します。たとえば、サブネットは 131.108.11.55 255.255.255.0 として表示されます。

ネットワーク マスクは、16 進数形式またはビット カウント形式で表示する方が便利なこともあります。16 進数形式は通常 UNIX システムで使用されます。前述の例の場合、131.108.11.55 0XFFFFFF00 として表示されます。

ビットカウント形式でネットワークマスクを表示すると、アドレス自体にスラッシュ (/) とネットマスクの合計ビット数が追加されます。前述の例の場合、131.108.11.55/24 として表示されま

現在のセッションにおけるネットマスク表示形式の指定

現在のセッションにおけるネットマスク表示形式を指定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **termipnetmask-format {bitcount | decimal | hexadecimal}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	termipnetmask-format {bitcount decimal hexadecimal} 例： Router# term ip netmask-format hexadecimal	ルータでのネットワーク マスクの表示に使用される形式を指定します。

個々の回線におけるネットマスク表示形式の指定

個々の回線におけるネットマスク表示形式を指定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **linevtyfirstlast**
4. **termipnetmask-format {bitcount | decimal | hexadecimal}**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	linevtyfirstlast 例： Router(config)# line vty 0 4	<i>first</i> および <i>last</i> 引数で指定した回線の範囲でライン 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	termipnetmask-format {bitcount decimal hexadecimal} 例： Router(config-line)# ip netmask-format hexadecimal	ルータで個々の回線のネットワーク マスクを表示するときに使用される形式を指定します。
ステップ 5	end 例： Router(config-if)# end	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ポイントツーポイント WAN インターフェイスの IP アンナンバードインターフェイスを使用することによる必要な IP アドレスの数の制限

ポイントツーポイント WAN インターフェイスの IP アンナンバードインターフェイスを使用することによる必要な IP アドレスの数の制限

IP ネットワークまたはサブネットアドレスの数が制限されていて、ネットワークでポイントツーポイント WAN を使用している場合、IP アンナンバードインターフェイス機能を使用することで、実際に IP アドレスを割り当てることなく、ポイントツーポイント WAN インターフェイスの IP 接続をイネーブルにできます。

ポイントツーポイント WAN インターフェイスで IP アンナンバードインターフェイス機能を設定するには、次の作業を実行します。

IP アンナンバード機能

IP アンナンバードインターフェイス機能を使用すると、明示的な IP アドレスに割り当てることなく、ポイントツーポイント WAN インターフェイスで IP 処理をイネーブルにできます。IP アンナンバードポイントツーポイント WAN インターフェイスは、別のインターフェイスの IP アドレスを使用して IP 接続をイネーブルにします。これにより、ネットワークアドレスを節約できます。



(注) IP アンナンバードインターフェイス機能には次の制約事項が適用されます。

- IP アンナンバードインターフェイス機能がサポートされるのは、ポイントツーポイント（非マルチアクセス）WAN インターフェイスだけです。
- IP アンナンバードインターフェイス機能を使用するインターフェイスで Cisco IOS イメージをネットブートできません。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `interfacetypenumber`
4. `noshutdown`
5. `ipaddressip-addressmask`
6. `interfacetypenumber`
7. `noshutdown`
8. `ipunnumberedtypenumber`
9. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interfacetypenumber 例： Router(config)# interface fastethernet 0/0	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	noshutdown 例： Router(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 5	ipaddressip-addressmask 例： Router(config-if)# ip address 172.16.16.1 255.255.240.0	インターフェイスの IP アドレスを設定します。
ステップ 6	interfacetypenumber 例： Router(config-if)# interface serial 0/0	ポイントツーポイント WAN インターフェイスを指定して、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	noshutdown 例： Router(config-if)# no shutdown	ポイントツーポイント WAN インターフェイスをイネーブルにします。

ポイントツーポイント WAN インターフェイスの 31 ビットプレフィックスの IP アドレスを使用することによる必要な IP アドレスの数の制限

	コマンドまたはアクション	目的
ステップ 8	ipunnumbered <i>typenumber</i> 例： <pre>Router(config-if)# ip unnumbered fastethernet 0/0</pre>	ポイントツーポイント WAN インターフェイスで IP アンナンバード機能をイネーブルにします。 この例では、ポイントツーポイント WAN インターフェイスは、ファストイーサネット 0/0 から IP アドレス 172.16.16.1 を使用します。
ステップ 9	end 例： <pre>Router(config-if)# end</pre>	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、IP アドレッシングのトラブルシューティングに役に立ちます。

- **showipinterface** : インターフェイスの IP パラメータを表示します。
- **showiprouteconnected** : ネットワーキングデバイスの接続先 IP ネットワークを表示します。

ポイントツーポイント WAN インターフェイスの 31 ビットプレフィックスの IP アドレスを使用することによる必要な IP アドレスの数の制限

ネットワーキングデバイスにより使用される IP サブネット数を削減して、RFC 3021 で規定されている 31 ビットプレフィックスの IP アドレスを使用して接続先のポイントツーポイント WAN との IP 接続を確立できます。

ポイントツーポイント WAN インターフェイスで 31 ビットプレフィックスの IP アドレスを設定するには、次の作業を実行します。

RFC 3021

RFC 3021 『*Using 31-bit Prefixes on IPv4 Point-to-Point Links*』より以前では、多くのネットワーク管理者は、30 ビットサブネットマスク (255.255.255.252) の IP アドレスをポイントツーポイント インターフェイスに割り当て、IP アドレス空間を節約していました。これにより、255.255.255.240 などのより短いサブネットマスクの IP アドレスを割り当てた場合よりも、IP アドレス空間を節約できましたが、30 ビットサブネットマスクの IP アドレスでは、リンクあたり 4 つのアドレスが必要です。これらは、ホストアドレスが 2 つ (リンクの各ホストインターフェイスに 1 つずつ

つ)、すべてゼロのネットワークアドレスが 1 つ、すべて 1 のブロードキャスト ネットワークアドレスが 1 つです。

次の表に、30 ビット (255.255.255.252 または /30) サブネット マスクが IP アドレス 192.168.100.4 に適用されるときに作成される 4 つの IP アドレスの例を示します。ホスト IP アドレスの指定に使用されるビットは太字で示しています。

表 8: 30 ビットサブネットマスク (/30) が使用されるときに作成される 4 つの IP アドレス

アドレス	説明	2 進数
192.168.100.4/30	すべてゼロの IP アドレス	11000000.10101000.01100100.00000 100
192.168.100.5/30	最初のホストアドレス	11000000.10101000.01100100.00000 101
192.168.100.6/30	2 番めのホストアドレス	11000000.10101000.01100100.00000 110
192.168.100.7/30	すべて 1 のブロードキャストアドレス	11000000.10101000.01100100.00000 111

ポイントツーポイントにはエンドポイント (ホスト) は 2 つだけで、一方のホストで転送される任意のパケットは、常にもう一方のホストで受信されるため、ブロードキャストサポートは必要ありません。そのため、すべて 1 のブロードキャスト IP アドレスは、ポイントツーポイントインターフェイスには必要ありません。

RFC 3021 を簡単に説明すると、31 ビットプレフィックス (31 ビットサブネットマスクを IP アドレスに適用されることで作成されます) を使用することで、ポイントツーポイントネットワークですべてゼロとすべて 1 の IP アドレスをホストアドレスとして割り当てることができます。RFC3021 より以前では、ポイントツーポイントリンクで一般的に使用される最長のプレフィックスは 30 ビットでした。つまり、すべてゼロとすべて 1 の IP アドレスは使用されていませんでした。

次の表に、31 ビット (255.255.255.254 または /31) サブネット マスクが IP アドレス 192.168.100.4 に適用されるときに作成される 2 つの IP アドレスの例を示します。ホスト IP アドレスの指定に使用されるビットは太字で示しています。

表 9: 31 ビットサブネットマスク (/31) が使用されるときに作成される 2 つの IP アドレス

アドレス	説明	2 進数
192.168.100.4/31	最初のホストアドレス	11000000.10101000.01100100.00000 100
192.168.100.5/31	2 番めのホストアドレス	11000000.10101000.01100100.00000 101

RFC 3021 の詳細については、<http://www.ietf.org/rfc/rfc3021.txt> を参照してください。

ポイントツーポイント WAN インターフェイスの 31 ビットプレフィックスの IP アドレスを使用すること
による必要な IP アドレスの数の制限

はじめる前に

31 ビットプレフィックスの IP アドレスをポイントツーポイント インターフェイスで設定する前に、クラスレス IP アドレッシングをネットワークデバイスで設定する必要があります。クラスレス IP アドレッシングは、Cisco IOS ソフトウェアの多くのバージョンでデフォルトでイネーブルにされています。ネットワーク デバイスで IP クラスレス アドレッシングが設定されているかわからない場合、グローバル コンフィギュレーション モードで **ipclassless** コマンドを入力して、クラスレス IP アドレッシングをイネーブルにします。



(注) この作業は、ポイントツーポイント（非マルチアクセス）WAN インターフェイスだけで実行できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipclassless**
4. **interfacetypenumber**
5. **noshutdown**
6. **ipaddressip-addressmask**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipclassless 例： Router(config)# ip classless	(任意) IP クラスレス (CIDR) をイネーブルにします。

	コマンドまたはアクション	目的
		(注) このコマンドは、Cisco IOS の多くのバージョンでデフォルトでイネーブルにされています。ネットワークデバイスを実行している Cisco IOS のバージョンでデフォルトでこのコマンドがイネーブルにされているかわからない場合、次に示すように ipclassless コマンドを入力します。この作業を実行したら、設定を表示します。 ipclassless コマンドが設定に表示されていない場合、デフォルトでイネーブルにされています。
ステップ 4	interface <i>typenumber</i> 例： Router(config)# interface serial 0/0	ポイントツーポイント WAN インターフェイスを指定して、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	no shutdown 例： Router(config-if)# no shutdown	インターフェイスをイネーブルにします。
ステップ 6	ip address <i>ip-addressmask</i> 例： Router(config-if)# ip address 192.168.100.4 255.255.255.254	31 ビットプレフィックスの IP アドレスをポイントツーポイント WAN インターフェイスで設定します。
ステップ 7	end 例： Router(config-if)# end	現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、IP アドレッシングのトラブルシューティングに役に立ちます。

- **show ip interface** : インターフェイスの IP パラメータを表示します。
- **show ip route connected** : ネットワーキングデバイスの接続先 IP ネットワークを表示します。

IP アドレスの設定例

例：IP アドレスをインターフェイスに割り当てることに起因する、ネットワークとの IP 接続の確立

次の例では、3つのインターフェイスで IP アドレスを設定します。

```
!  
interface FastEthernet0/0  
no shutdown  
ip address 172.16.16.1 255.255.240.0  
!  
interface FastEthernet0/1  
no shutdown  
ip address 172.16.32.1 255.255.240.0  
!  
interface FastEthernet0/2  
no shutdown  
ip address 172.16.48.1 255.255.240.0  
!
```

例：セカンダリ IP アドレスの使用によるネットワークでサポートされる IP ホストの数の増加

次の例では、3つのインターフェイスでセカンダリ IP アドレスを設定します。

```
!  
interface FastEthernet0/0  
no shutdown  
ip address 172.16.16.1 255.255.240.0  
ip address 172.16.32.1 255.255.240.0 secondary  
!  
!  
interface FastEthernet0/1  
no shutdown  
ip address 172.17.16.1 255.255.240.0  
ip address 172.17.32.1 255.255.240.0 secondary  
!  
!  
interface FastEthernet0/2  
no shutdown  
ip address 172.18.16.1 255.255.240.0  
ip address 172.18.32.1 255.255.240.0 secondary  
!
```

例：ポイントツーポイント WAN インターフェイスの IP アンナンバード インターフェイスを使用することによる必要な IP アドレスの数の制限

次の例では、3つのインターフェイスでアンナンバード IP 機能を設定します。

```
!  
interface FastEthernet0/0  
  no shutdown  
  ip address 172.16.16.1 255.255.240.0  
!  
interface serial0/0  
  no shutdown  
  ip unnumbered fastethernet0/0  
!  
interface serial0/1  
  no shutdown  
  ip unnumbered fastethernet0/0  
!  
interface serial0/2  
  no shutdown  
  ip unnumbered fastethernet0/0  
!
```

例：ポイントツーポイント WAN インターフェイスの 31 ビット プレフィックスの IP アドレスを使用することによる必要な IP アドレスの数の制限

次の例では、2つのインターフェイスで 31 ビット プレフィックスを設定します。

```
!  
ip classless  
!  
interface serial0/0  
  no shutdown  
  ip address 192.168.100.2 255.255.255.254  
!  
!  
interface serial0/1  
  no shutdown  
  ip address 192.168.100.4 255.255.255.254
```

例：IP サブネット ゼロの使用を許可することによる、使用可能な IP サブネット数の最大化

次の例では、サブネット ゼロをイネーブルにします。

```
!  
interface FastEthernet0/0  
  no shutdown  
  ip address 172.16.16.1 255.255.240.0  
!
```

```
ip subnet-zero
!
```

次の作業

ネットワークに複数のルータがあり、ルーティングプロトコルを設定していない場合、ルーティングプロトコルの設定については、『Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T』を参照してください。

その他の参考資料

関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
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 ISBN 1578701082』

標準規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	--

MIB

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

RFC

RFC ⁶	タイトル
RFC 791	『Internet Protocol』 http://www.ietf.org/rfc/rfc0791.txt
RFC 1338	『Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy』 (http://www.ietf.org/rfc/rfc1519.txt)
RFC 1466	『Guidelines for Management of IP Address Space』 (http://www.ietf.org/rfc/rfc1466.txt)
RFC 1716	『Towards Requirements for IP Routers』 (http://www.ietf.org/rfc/rfc1716.txt)
RFC 1918	『Address Allocation for Private Internets』 (http://www.ietf.org/rfc/rfc1918.txt)
RFC 3330	『Special-Use IP Addresses』 (http://www.ietf.org/rfc/rfc3330.txt)

⁶ これらの参考資料は、IP アドレッシングおよび IP ルーティングに関連する項目で使用可能な多くの RFC の例です。RFC の完全なリストについては、IETF RFC のサイト (<http://www.ietf.org/rfc.html>) を参照してください。

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、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 アドレスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

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

表 10: IP アドレスの機能情報

機能名	リリース	機能情報
Classless Inter-Domain Routing	10.0	CIDR は、クラス（クラス A、クラス B など）の概念をなくす、新しい IP アドレスの参照方法です。たとえば、ネットワーク 192.213.0.0（不正なクラス C ネットワーク番号）は、CIDR 表記で 192.213.0.0/16 と表される場合、有効なスーパーネットです。/16 は、スーパーネットマスクが 16 ビットで構成されることを示します（左からカウントします）。そのため、192.213.0.0/16 は、192.213.0.0 255.255.0.0 と同じです。 次のコマンドが導入または変更されました。 ipclassless 。
IP サブネット ゼロ	10.0	IP アドレス空間を節約するために、IP サブネット ゼロにより、インターフェイスの IP アドレスとしてすべてゼロのサブネットを使用できます。たとえば、ファストイーサネット 0/0 で 172.16.0.1/24 を設定できます。 次のコマンドが導入または変更されました。 ipsubnet-zero 。

機能名	リリース	機能情報
IP アンナンバード インターフェイス	10.0	IP アドレス空間を節約するために、IP アンナンバード インターフェイスは、別のインターフェイスの IP アドレスを使用して IP 接続を確立できます。 次のコマンドが導入または変更されました。 ipunnumbered 。
IP ポイントツーポイント リンクでの 31 ビットプレフィックスの使用	12.0(14)S 12.2(4)T	インターネットで IP アドレス空間を節約するために、31 ビットプレフィックス長により、ポイントツーポイント リンクで 2 つだけの IP アドレスの使用が可能になりました。以前は、カスタマーは、ポイントツーポイント リンクで IP アドレスまたはアンナンバード インターフェイスを 4 つ使用する必要がありました。



第 3 章

IP オーバーラッピング アドレス プール

IP オーバーラッピングアドレスプール機能を使用すると、ダイナミック IP アドレス割り当ての柔軟性が向上します。この機能を使用すると、オーバーラッピング IP アドレスプールグループを設定して、異なるアドレス空間を作成し、異なるアドレス空間で同じ IP アドレスを同時に使用できます。

- [機能情報の確認, 35 ページ](#)
- [IP オーバーラッピングアドレスプールの制約事項, 36 ページ](#)
- [自動 IP オーバーラッピングアドレスプールに関する情報, 36 ページ](#)
- [IP オーバーラッピングアドレスプールの設定方法, 37 ページ](#)
- [IP オーバーラッピングアドレスプールの設定の設定例, 38 ページ](#)
- [その他の参考資料, 38 ページ](#)
- [IP オーバーラッピングアドレスプールの設定の機能情報, 40 ページ](#)
- [用語集, 41 ページ](#)

機能情報の確認

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

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

IP オーバーラッピングアドレス プールの制約事項

Cisco IOS XE ソフトウェアでは、グループ単位で重複アドレスをチェックします。重複アドレスのチェックは、重複するアドレスを含むことのある複数のグループ内にプールを設定できることを示しています。IP オーバーラッピングアドレスプール機能は、複数の IP アドレス空間がサポートされているマルチプロトコル 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) 環境など、オーバーラッピング IP アドレスプールが有効な場合のみ使用する必要があります。

自動 IP オーバーラッピングアドレス プールに関する情報

利点

IP オーバーラッピングアドレス プールによって、ダイナミック IP アドレス割り当てをより柔軟に実行できます。この機能を使用すると、オーバーラッピング IP アドレス プール グループを設定して、異なるアドレス空間を作成し、異なるアドレス空間で同じ IP アドレスを同時に使用できます。

IP アドレス グループの仕組み

IP Control Protocol (IPCP) IP プール処理では、単一の IP アドレス空間に属するようにすべての IP アドレスが実装されます。特定の IP アドレスを複数回割り当てることはできません。バーチャルプライベートダイヤルアップネットワーク (VPDN)、ネットワークアドレス変換 (NAT) などの IP 開発では、IP アドレスを再使用するために意味を持つ複数 IP アドレス空間の概念が実装されています。ただし、そのような使用法では、これらの重複アドレスが同じ IP アドレス空間に配置されていないことを確認する必要があります。複数の IP アドレス空間をサポートし、かつ、プールグループ内で非オーバーラッピング IP アドレス プールの検証を可能にするのが IP アドレスグループです。プール名はルータ内で一意である必要があります。プール名を関連付けることができるのは 1 つのグループだけであるため、プール名には暗黙グループ識別子が含まれていません。明示グループ名なしのプールは、ベース システム グループのメンバーと見なされ、元の IP プール実装と同じ方法で処理されます。

新しいプール機能によって既存の設定が影響を受けることはありません。「グループ」の概念は、既存の `ip local pool` コマンドの拡張です。グループのメンバーとして指定されていないプールの処理は、既存の実装から変更されていません。

IP オーバーラッピングアドレス プールの設定方法

ローカル プール グループの設定および確認

ローカルプールグループを設定し、グループが存在していることを確認するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `iplocalpool{default | poolname} {low-ip-address [high-ip-address] [group group-name] [cache-size size]}`
4. `showiplocalpool [poolname | [group group-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	イネーブル化 例： Router> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>configureterminal</code> 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	<code>iplocalpool{default poolname} {low-ip-address [high-ip-address] [group group-name] [cache-size size]}</code> 例： Router(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000	ローカル IP アドレス プールのグループを設定し、このグループに名前とキャッシュ サイズを指定します。
ステップ 4	<code>showiplocalpool [poolname [group group-name]]</code> 例： Router(config)# show ip local pool group testgroup testpool	定義済みの IP アドレス プールすべての統計情報を表示します。

IP オーバーラッピングアドレス プールの設定の設定例

グローバル デフォルト メカニズムとしてのローカル アドレス プーリングの定義例

次の例は、ローカル プールをグローバル デフォルト メカニズムとして設定する方法を示しています。

```
ip address-pool local
ip local pool default 192.168.15.15 192.168.15.16
```

複数範囲の IP アドレスの単一プールへの設定例

次の例は、2つの範囲の IP アドレスを1つの IP アドレス プールに設定する方法を示しています。

```
ip local pool default 192.169.10.10 192.169.10.20
ip local pool default 192.168.50.25 192.168.50.50
```

その他の参考資料

ここでは、IP オーバーラッピングアドレスプールの設定に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
ダイヤルコマンド：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 Dial Services Command Reference』
IP アドレス プーリング	『Cisco IOS XE Dial Technologies Configuration Guide』の「Configuring Media-Independent PPP and Multilink PPP」の章

標準規格

標準規格	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

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

RFC

RFC	タイトル
RFC 826	『 <i>Address Resolution Protocol</i> 』
RFC 903	『 <i>Reverse Address Resolution Protocol</i> 』
RFC 1027	『 <i>ProxyAddress Resolution Protocol</i> 』
RFC 1042	『 <i>Standard for the Transmission of IP Datagrams over IEEE 802 Networks</i> 』

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <p>シスコのサポート Web サイトのツールにアクセスする場合、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/en/US/support/index.html</p>

IP オーバーラッピングアドレス プールの設定の機能情報

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

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

表 11: IP オーバーラッピングアドレス プールの設定の機能情報

機能名	リリース	機能情報
IP オーバーラッピングアドレス プール	Cisco IOS XE Release 2.1	<p>IP オーバーラッピングアドレス プール機能を使用すると、ダイナミック IP アドレス割り当ての柔軟性が向上します。この機能を使用すると、オーバーラッピング IP アドレス プールグループを設定して、異なるアドレス空間を作成し、異なるアドレス空間で同じ IP アドレスを同時に使用できます。</p> <p>この機能により、次のコマンドが変更されました。</p> <p>iplocalpool、showiplocalpool。</p>

用語集

IPCP : IP Control Protocol。PPP を介して IP を確立および設定するプロトコルです。

MPLS : マルチプロトコルラベルスイッチング。ラベルを使用して IP トラフィックを転送するスイッチング方式。このラベルによって、ネットワーク内のルータおよびスイッチが、事前に確立された IP ルーティング情報に基づくパケットの転送先を指示されます。

NAT : ネットワークアドレス変換 (NAT) 。グローバルに固有な IP アドレスを使用する必要性を減らすメカニズムです。NAT を使用すると、グローバルに一意ではないアドレスを持つ組織が、それら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することで、インターネットに接続できるようになります。ネットワークアドレストランスレータとも呼ばれています。

VPDN : バーチャルプライベートダイヤルアップネットワーク。バーチャルプライベートダイヤルネットワークとも呼ばれます。VPDN は、共有インフラストラクチャを使用してプライベートネットワークまでリモートアクセスを拡張するネットワークです。VPDN では、レイヤ 2 トンネルテクノロジー (L2F、L2TP、PPTP) を使用して、レイヤ 2 およびネットワーク接続の上位部分を、リモートユーザから ISP ネットワークをまたがってプライベートネットワークまで拡張します。VPDN は、リモートダイヤルユーザとプライベートネットワーク間に長距離のポイントツーポイント接続を確立するコスト効率の高い方法です。「VPN」も参照。

VPN : バーチャルプライベートネットワーク。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

VRF : VPN ルーティングおよび転送インスタンス。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、

ルーティングテーブルに登録されるものを決定する一連のルールおよびルーティングプロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。



第 4 章

自動 IP アンナンバードイーサネットポーリングのサポート

IP アンナンバードイーサネットポーリングサポート機能は、イーサネット物理インターフェイス用の IP アンナンバードサポートを提供します。このサポートは、シリアルインターフェイス用にすでに存在します。

- [機能情報の確認, 43 ページ](#)
- [IP アンナンバードイーサネットポーリングのサポートに関する情報, 44 ページ](#)
- [IP アンナンバードイーサネットポーリングのサポートの設定方法, 44 ページ](#)
- [IP アンナンバードイーサネットポーリングのサポートの設定例, 48 ページ](#)
- [その他の参考資料, 49 ページ](#)
- [IP アンナンバードイーサネットポーリングのサポートの機能情報, 49 ページ](#)

機能情報の確認

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

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

IP アンナンバードイーサネットポーリングのサポートに関する情報

自動 IP アンナンバードイーサネットポーリングサポートの概要

シリアルインターフェイス用の IP アンナンバードサポートがイーサネット物理インターフェイスまで拡張されています。アンナンバードイーサネット物理インターフェイスは、アンナンバードシリアルインターフェイスと同様に使用されます。1 台のデバイス上で、ループバックインターフェイスが設定されており、IP アドレスがこのインターフェイスに割り当てられている場合、複数のイーサネット物理インターフェイスでのポーリングオプションの使用は、ループバックに対してアンナンバードにすることができます。

ポーリングオプションによって、Address Resolution Protocol (ARP) プロトコルに基づくホストの動的な検出 (アンナンバードインターフェイスを介して接続) が可能になります。

IP アンナンバードイーサネットポーリングのサポートの設定方法

イーサネットインターフェイスのポーリングのイネーブル化

手順の概要

1. イネーブル化
2. `configureterminal`
3. `interfacetypenumber`
4. `ipaddressip-addressmask`
5. `exit`
6. `interfacetypenumber`
7. `ipunnumberedtypenumberpoll`
8. `end`

手順の詳細

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

	コマンドまたはアクション	目的
	例 : Device> enable	<ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 例 : Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	interface <i>typenumber</i> 例 : Device(config)# interface loopback 0	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ipaddress <i>ip-addressmask</i> 例 : Device(config-if)# ip address 209.165.200.229 255.255.240.224	インターフェイスの IP アドレスを設定します。
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戻ります。
ステップ 6	interface <i>typenumber</i> 例 : Device(config)# interface ethernet 0/0	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	ipunnumbered <i>typenumberpoll</i> 例 : Device(config-if)# ip unnumbered loopback 0 poll	指定されたインターフェイス上で IP 接続ホストのポーリングをイネーブルにします。
ステップ 8	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。

アンナバードインターフェイスの IP ARP ポーリング用のキューのサイズとパケットレートの設定

手順の概要

1. イネーブル化
2. `configureterminal`
3. `iparpollqueuequeue-size`
4. `iparpollratepacket-rate`
5. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>configureterminal</code> 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	<code>iparpollqueuequeue-size</code> 例： Device(config)# ip arp poll queue 1000	IP ARP ポーリング キューのサイズを設定します。
ステップ 4	<code>iparpollratepacket-rate</code> 例： Device(config)# ip arp poll rate 1000	IP ARP ポーリング パケットレートをパケット/秒単位で設定します。
ステップ 5	<code>end</code> 例： Device(config-if)# end	特権 EXEC モードに戻ります。

IP アンナンバードイーサネットポーリングサポートの確認

IP アンナンバードイーサネットポーリングサポートを確認するには、次の作業を実行します。



(注) **show** コマンドに、特定の順序はありません。

手順の概要

1. イネーブル化
2. **show ip arp poll**
3. **show ip interface type number unnumbered**
4. **show ip interface type number unnumbereddetail**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

例：
Device> **enable**

ステップ 2 **show ip arp poll**

IP ARP ホストポーリングのステータスを表示します。

例：
Device# **show ip arp poll**

```
Number of IP addresses processed for polling: 438
Number of entries in the queue: 100 (high water mark: 154, max: 1000)
Number of request dropped:
  Queue was full: 1288
  Request was throttled by incomplete ARP: 10
  Duplicate entry found in queue: 1431
```

ステップ 3 **show ip interface type number unnumbered**

IP 用に設定されたインターフェイスのアンナンバードインターフェイスサポートのステータスを表示します。

例：
Device# **show ip interface loopback 0 unnumbered**

```
Number of unnumbered interfaces with polling: 10
Number of IP addresses processed for polling: 15
Number of IP addresses in queue for polling: 4
```

ステップ 4 show ip interface type number unnumbereddetail

IP 用に設定されたインターフェイスのアンナンバードインターフェイス サポートの詳細ステータスを表示します。

例：

```
Device# show ip interface loopback 0 unnumbered detail

Number of unnumbered interfaces with polling: 10
Number of IP addresses processed for polling: 15
Last 10 IP addresses processed for polling:
 209.165.201.2
 209.165.201.3
 209.165.201.4
 209.165.201.5
 209.165.201.6
 209.165.201.7
 209.165.201.8
 209.165.201.9
 209.165.201.10
 209.165.201.11
Number of IP addresses in queue for polling: 4 (high water mark: 5)
 209.165.201.12
 209.165.201.13
 209.165.201.14
 209.165.201.15
```

IP アンナンバードイーサネットポーリングのサポートの設定例

例：イーサネット インターフェイスのポーリングのイネーブル化

```
Device> enable
Device# configure terminal
Device(config)# interface loopback 0
Device(config-if)# ip address 209.165.200.229 255.255.240.224
Device(config-if)# exit
Device(config)# interface ethernet 0/0
Device(config-if)# ip unnumbered loopback 0 poll
Device(config-if)# end
```

例：アンナンバードインターフェイスのIPARPポーリング用のキューのサイズとパケット レートの設定

```
Device> enable
Device# configure terminal
Device(config)# ip arp poll queue 1000
Device(config)# ip arp poll rate 1000
```

Device(config)# end

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPv4 アドレッシング コマンド	『Cisco IOS IP Addressing Services Command Reference』
IPv4 アドレスに関する概念情報	『IP Addressing: IPv4 Addressing Configuration Guide』内の「Configuring IPv4 Addresses」モジュール

シスコのテクニカル サポート

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

IP アンナナバードイーサネットポーリングのサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレー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: IP アンナナバード イーサネット ポーリングのサポートの機能情報

機能名	リリース	機能情報
自動 IP アンナナバード イーサネット ポーリングのサポート	Cisco IOS XE Release 3.8S	<p>IP アンナナバード イーサネット ポーリング サポート機能は、イーサネット物理インターフェイス用の IP アンナナバード サポートを提供します。</p> <p>次のコマンドが導入または変更されました。</p> <p>cleariparppollstatistics、 clearipinterface、iparppoll、 ipunnumberedpoll、 showiparppoll、 showipinterfaceunnumbered。</p>



第 5 章

自動 IP

自動 IP 機能では、リングに挿入されたノードに IP アドレスを自動的に提供します。リングトポロジでは、デバイスがリングに挿入される場合、ネイバー ノード インターフェイスで手動再設定が必要です。自動 IP 機能では、リング内のノードの挿入、削除、移動に伴うノードの手動再設定の問題に対処します。自動 IP 機能は以下でサポートされています。

- イーサネット インターフェイスとサブ インターフェイス。
- Virtual Routing and Forwarding (VRF) インスタンス インターフェイス。
- スイッチ仮想インターフェイス (SVI) 。
- EtherChannel。



注 VRF インターフェイス、SVI、および EtherChannel 上で自動 IP 機能をサポートするリリースバージョンを確認するには、[自動 IP の機能情報](#)を参照してください。



(注) デバイスはリングに挿入されると、ノードと呼ばれます。

- [機能情報の確認](#), 52 ページ
- [自動 IP の前提条件](#), 52 ページ
- [自動 IP の制約事項](#), 52 ページ
- [自動 IP に関する情報](#), 53 ページ
- [自動 IP の設定方法](#), 62 ページ
- [自動 IP の設定例](#), 69 ページ
- [自動 IP に関する追加情報](#), 69 ページ
- [自動 IP の機能情報](#), 70 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、[Bug Search Tool](#) およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

自動 IP の前提条件

- ノードインターフェイスで自動 IP 機能をイネーブルにする前に、Link Layer Discovery Protocol (LLDP) がデバイスでイネーブルにされている必要があります。

EtherChannel 上の自動 IP

- EtherChannel 上で自動 IP を設定するときは、LLDP が EtherChannel のメンバー インターフェイス上でイネーブルになっていることを確認してください。
- インターフェイス上の自動 IP 設定は、EtherChannel にインターフェイスを移動する前に削除する必要があります。

VRF インターフェイス上の自動 IP

- 特定の Virtual Routing and Forwarding (VRF) インスタンス用にインターフェイス上に自動 IP を設定する場合は、インターフェイスが現在 VRF 内に存在していることを確認してください。インターフェイス上の自動 IP をイネーブルにした後にインターフェイスを VRF に関連付けると、インターフェイス上の自動 IP 設定はクリアされるため、VRF インターフェイス上で自動 IP 機能を再度イネーブルにする必要があります。

自動 IP の制約事項

- 自動 IP アドレスは最後のオクテットに偶数を含むことはできません（たとえば、10.1.1.2 の最後のオクテットの値は 2）。

VRF インターフェイス上の自動 IP

- インターフェイス上の自動 IP 設定は、グローバル VRF を含め、Virtual Routing and Forwarding (VRF) インスタンス間でインターフェイスが移動されるときに維持されません。

- 異なる VRF 内のインターフェイス ノードは、同じリング用に設定できません。選択する複数のノードが同じ VRF に属していることを確認してください。
- VRF のアドレスファミリーが IPv6 である場合、VRF 内のインターフェイス上に自動 IP を設定できません。VRF のアドレスファミリー IPv4 であれば、VRF インターフェイス上に自動 IP アドレスを設定できます。

SVI インターフェイス上の自動 IP

- 自動 IP 設定は、複数の物理インターフェイスを備えたスイッチ仮想インターフェイス (SVI) 上では不可能です。SVI 物理インターフェイスは、関連付けられた VLAN またはブリッジドメインインターフェイス (BDI) が 1 つのみのアクセスポートまたはトランクポートである必要があります。

EtherChannel インターフェイス上の自動 IP

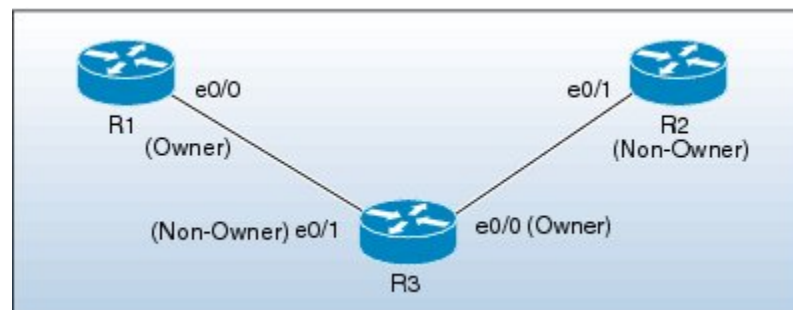
- 自動 IP 設定を EtherChannel インターフェイス上で実施することはできますが、EtherChannel メンバーインターフェイス上ではできません。

自動 IP に関する情報

自動 IP の概要

自動 IP 機能は、Link Layer Discovery Protocol (LLDP) を強化したプロトコルです。LLDP は、ネイバー デバイスの検出に属性セットを使用します。この属性セットは、タイプ、長さ、および値の記述を含んでいるため、タイプ/長さ/値 (TLV) と呼ばれます。

リング トポロジでは、デバイスの 2 つのネットワーク間インターフェイス (NNI または ノード インターフェイス) がリングの一部として使用されます。リングが自動 IP リングとして機能するためには、リング内のすべてのノード インターフェイス上に自動 IP 機能を設定する必要があります。デバイスのいずれかのノード インターフェイスがオーナー インターフェイスとして指定され、他のインターフェイスは非オーナー インターフェイスとして指定されます。自動 IP リング内では、デバイスのオーナー インターフェイスは、ネイバー デバイスの非オーナー インターフェイスに接続されます。トポロジ例は次のとおりです。



新しいデバイスが自動 IP リングに挿入されると、挿入されたデバイスのオーナーと非オーナーのインターフェイスが識別されます。オーナーインターフェイスに接続されている、挿入されたデバイスのノードインターフェイスは非オーナーインターフェイスとして指定され、接続されたネイバー デバイスから IP アドレスを自動的に受け取ります。IP アドレスはインターフェイス上に自動的に設定されます。非オーナーインターフェイスが識別されたので、挿入されたデバイスの他のノードインターフェイスはオーナーインターフェイスとして指定され、デバイスは事前設定された自動 IP アドレスを指定されたオーナー インターフェイスに割り当てます。

自動 IP アドレスとは、自動 IP リング内で検出された新しいネイバーインターフェイスにインターフェイスで IP アドレスを自動で割り当てることができるように、ノードインターフェイス上に設定された事前設定されたアドレスです。設定された自動 IP アドレスは割り当てを行うために使用されます。

自動 IP リングの一部として指定される 2 つのノードインターフェイス上に同じ自動 IP アドレスを設定する必要があり、自動 IP アドレスは最後のオクテットに奇数を含んでいる必要があります。自動 IP アドレスは、デバイスが自動 IP リングに導入されたときにオーナー インターフェイスに割り当てられます。それぞれの自動 IP アドレスは最後のオクテットに奇数を含んでいるため、最後のオクテットから 1 を引いて得られる IP アドレスは偶数であり、自動 IP アドレスを指定するために使用されません。この IP アドレスは、新たに検出されたネイバーの非オーナーインターフェイスに割り当てられます。

たとえば、上のトポロジで、R1 と R2 の間にデバイス R3 が挿入され、自動 IP アドレス 10.1.1.3 がデバイス R3 上の 2 つのノードインターフェイス e0/1 と e0/0 に設定されていると仮定すると、R1 では、R3 の非オーナー インターフェイス e0/1 に IP アドレスを割り当てます。IP アドレス 10.1.1.3 が R3 のオーナー インターフェイス e0/0 に割り当てられます。自動 IP アドレスの最後のオクテットから 1 を引くことで取得される IP アドレスは 10.1.1.2 です。10.1.1.2 は、接続されたネイバー デバイス R2 のネイバー非オーナー インターフェイスに割り当てられます。

自動 IP TLV 交換

挿入前、ノードインターフェイスは、オーナーと非オーナーのいずれとしても指定されていません。挿入後は、自動 IP TLV がネイバー デバイス間で交換されます。隣接するデバイス インターフェイスとのこの初期ネゴシエーション中に、オーナーと非オーナーのインターフェイスが自動的に判別されます。

デバイスがリングに挿入されると、デバイスに設定された自動 IP アドレス（10.1.1.3 など）が、/31 サブネット用のオーナーインターフェイスに割り当てられます。オーナーインターフェイスは自動 IP TLV 内でプライオリティ 2 を持ち、非オーナーインターフェイスは自動 IP TLV 内でプライオリティ 0 を持ちます。（ノードがリングに挿入される前の時点で）ノードインターフェイスに割り当てられた IP アドレスが存在しない場合、リング インターフェイスは自動 IP TLV 内でプライオリティ 1 を持ちます。

IP アドレスのネゴシエーションはプライオリティに基づきます。プライオリティの値が大きいとネゴシエーションで選択されます。プライオリティが等しければ、IP ネゴシエーションは失敗します。このシナリオは、通常、設定または配線が正しくないときに発生します。このようなシナリオでは、設定および配線が適切であることを確認する必要があります。

VRF インターフェイス上の自動 IP

Virtual Routing and Forwarding (VRF) インスタンス インターフェイス上の自動 IP 設定におけるいくつかのポイントを以下に示します。

- インターフェイス上の自動 IP 設定は、グローバル VRF を含め、インターフェイスが VRF 間で移動されるときに削除されます。したがって、インターフェイスを VRF に割り当てた後に、インターフェイス上で自動 IP 機能を設定します。
- VRF インターフェイス上に自動 IP を設定できるのは、VRF のアドレス ファミリが IPv4 である場合のみです。IPv4 アドレス ファミリ構成が VRF から削除されると、自動 IP 構成が VRF 内のすべてのインターフェイスから削除されます。
- VRF のアドレス ファミリが IPv6 である場合、VRF 内のインターフェイス上に自動 IP を設定できません。ただし、VRF のアドレス ファミリが IPv4 と IPv6 である場合は、VRF 内のインターフェイス上に自動 IP を設定できます。
- IPv4 と IPv6 の両アドレス ファミリ構成を持つ VRF から IPv6 アドレス ファミリ構成が削除される場合、VRF 内のインターフェイス上の自動 IP 設定はそのまま維持されます。
- VRF が削除されると、VRF に割り当てられているすべてのインターフェイス上の自動 IP 設定が削除されます。
- リングごとに 2 つのインターフェイス ノードがあります。選択する 2 つのノードが同じ VRF に属していることを確認してください。異なる VRF 内のノードは、同じリング用に設定できません。
- VRF 内では、同じ自動 IP アドレスを異なるリング ID に使用できません。

EtherChannel インターフェイス上の自動 IP

EtherChannel インターフェイスの自動 IP 設定におけるいくつかのポイントを以下に示します。

- EtherChannel インターフェイス上に自動 IP を設定できます。EtherChannel 上に自動 IP 機能を設定した後にこの EtherChannel にメンバー インターフェイスを追加すると、自動 IP TLV 情報がすべてのメンバー インターフェイスに伝送されます。EtherChannel にメンバー インターフェイスを追加した後に EtherChannel 上で自動 IP を設定すると、自動 IP TLV 情報はすべてのメンバー インターフェイスに伝送されます。



注目 LLDP がメンバー インターフェイス上でイネーブルである必要があります。

- EtherChannel メンバー インターフェイスの一覧は、EtherChannel に対応するリング インターフェイス内で維持されます。自動 IP 情報は、すべての EtherChannel メンバー インターフェイス上で送信されます。
- EtherChannel からメンバー インターフェイスを削除する場合、自動 IP TLV 情報は削除されたインターフェイスに伝送されません。

SVI インターフェイス上の自動 IP

スイッチ仮想インターフェイス (SVI) 上の自動 IP 設定におけるいくつかのポイントを以下に示します。

- SVI 上の自動 IP 設定は、単一の物理インターフェイスが SVI に関連付けられているときだけ可能です。
- SVI 物理インターフェイスは、関連付けられた VLAN またはブリッジドメインインターフェイス (BDI) が 1 つのみのアクセスポートまたはトランクポートである必要があります。
- SVI が複数の物理ポートにマッピングされると、SVI 上の自動 IP 設定は削除されます。

Seed Device

シードデバイスはネットワーク検出を開始するために使用されるデバイスです。リング内で自動 IP 機能を開始するには、少なくとも 1 台のデバイスをリング内のシードデバイスとして設定する必要があります。自動 IP リング内でシードデバイスとしてデバイスを設定するには、いずれかのノードインターフェイスに設定されている IP アドレスに、マスク /31 (または 255.255.255.254) を付けたインターフェイスの自動 IP アドレスを手動で設定する必要があります。

トポロジ例は次のとおりです。このシナリオでは、デバイス R1 がシードデバイスとして設定されています。



デバイス R1 上の e0/0 インターフェイスには自動 IP アドレス 10.1.1.1 が設定され、デバイス R2 上の e0/1 インターフェイスには自動 IP アドレス 10.1.1.3 が設定されています。

シードデバイスとして R1 を設定するには、10.1.1.1 がインターフェイス e0/0 の IP アドレスとして設定されている必要があります。R1 の e0/0 インターフェイスの IP アドレスを自動 IP アドレスに設定することで、R1 はシードデバイスとして設定され、インターフェイス e0/0 がサブネットのオーナーになります。

シードデバイスとしてデバイス R1 を設定するプロセスについては、次に示します。

デバイス R1 と R2 の間に接続が確立された後に、R1 はプライオリティ 2 の自動 IP タイプ/長さ/値 (TLV) を含む Link Layer Discovery Protocol (LLDP) パケットを送信します。

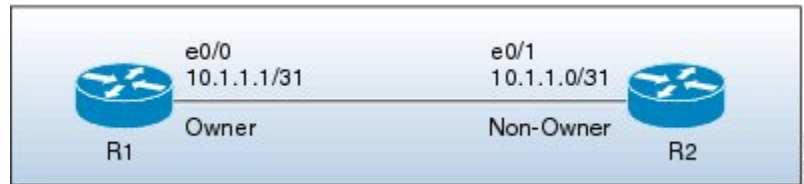
R1 上の e0/0 インターフェイスの自動 IP 情報を次に示します。

インターフェイス IP アドレス	自動 IP アドレス	プライオリティ
10.1.1.1	10.1.1.1	2

R1 から自動 IP TLV を受信すると、R2 はインターフェイス e0/1 用の IP アドレスを取得し (R1 の自動 IP アドレスの最後のオクテットから 1 を減算)、IP アドレス 10.1.1.0/31 を R2 の e0/1 イン

ターフェイスに割り当てます。R2 上のインターフェイス e0/1 はこのサブネット上の非オーナーインターフェイスになります。

IP アドレスの割り当てを、次に示す図に示します。



サブネットのデバイスおよびノードインターフェイスの詳細を次に示します。

デバイス	インターフェイス	IP アドレス	名称
R1	e0/0	10.1.1.1/31	オーナー
R2	e0/1	10.1.1.0/31	非オーナー



- (注) R2 上の e0/1 インターフェイス上に設定されている自動 IP アドレスは 10.1.1.3 であるため、R2 のもう一方のノードインターフェイスがオーナーインターフェイスとして指定され、10.1.1.3 がもう一方のノードインターフェイスのインターフェイス IP アドレスとして自動的に設定されます。

自動 IP リングにデバイスを挿入するための自動 IP 設定

既存の自動 IP リングにデバイスを挿入するには、デバイスのノードインターフェイスに自動 IP アドレスが設定されている必要があります。



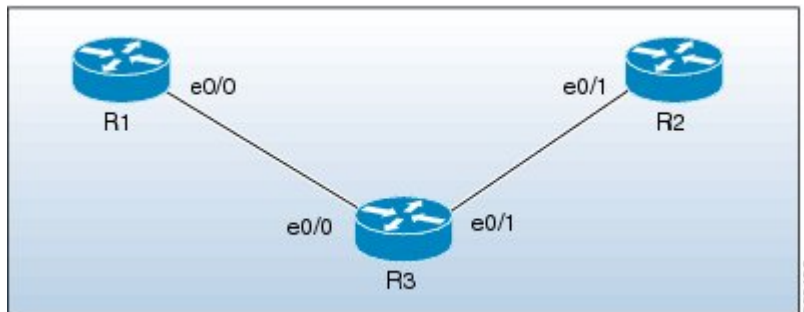
- (注) 既存の一部である一方で自動 IP リングでないノードインターフェイス上に自動 IP 機能を設定することもできます。

下の図のトポロジはシナリオ例を示しています。



デバイス R1 はシードデバイスとして設定されています。R1 上のインターフェイス e0/0 は IP アドレス 10.1.1.1/31 で設定されており、R1 と R2 を接続するサブネットのオーナーです。デバイス R2 上のインターフェイス e0/1 は IP アドレス 10.1.1.0/31 を持ち、サブネットの非オーナーインターフェイスです。

デバイス R3 は R1 と R2 の間に挿入されています。R3 の 2 つの指定ノードインターフェイス e0/0 と e0/1 は、自動 IP アドレス 10.1.1.5 で設定されます。デバイスを挿入すると、リングトポロジは下の図のように表示されます。



デバイス R1 と R3 の間の自動 IP TLV 交換を次に示します。

- 1 R1 は R3 の e0/0 インターフェイスにプライオリティ 2 の自動 IP タイプ/長さ/値 (TLV) を送信します。
- 2 R1 から自動 IP TLV を受信した後、R3 は R1 の e0/0 インターフェイスにプライオリティ 0 の自動 IP TLV を送信します。
- 3 R1 は選択プロセスによって選択され、R1 のインターフェイス e0/0 が R1 と R3 を接続するサブネット上のオーナー インターフェイスとして指定されます。
- 4 R3 上の e0/0 インターフェイスは非オーナー インターフェイスになり、IP アドレス 10.1.1.0 が割り当てられます。
- 5 R3 上のもう一方のノードインターフェイスはオーナー インターフェイスとして指定され、このインターフェイスの自動 IP アドレス (10.1.1.5) がインターフェイスの IP アドレスとして割り当てられます。

デバイス R3 と R2 の間の自動 IP TLV 交換を次に示します。

- 1 R3 はプライオリティ 2 の自動 IP TLV を R2 上の e0/1 インターフェイスに送信します。
- 2 R3 から自動 IP TLV を受信した後、R2 は R3 の e0/1 インターフェイスにプライオリティ 0 の自動 IP TLV を送信します。
- 3 R3 は選択プロセスによって選択され、R3 のインターフェイス e0/1 が R3 と R2 を接続するサブネット上のオーナー インターフェイスとして指定されます。
- 4 R2 上の e0/1 インターフェイスが非オーナー インターフェイスとして指定され、IP アドレス 10.1.1.4 が割り当てられます。
- 5 R2 上のもう一方のノードインターフェイスはオーナー インターフェイスとして指定され、このインターフェイスの自動 IP アドレスが IP アドレスとして割り当てられます。

デバイス R1、R2、R3 のオーナーと非オーナーのインターフェイスに設定されている IP アドレスを次に示します。

デバイス	インターフェイス	IP Address	名称
------	----------	------------	----

R1	e0/0	10.1.1.1/31	オーナー
R3	e0/0	10.1.1.0/31	非オーナー
R3	e0/1	10.1.1.5/31	オーナー
R2	e0/1	10.1.1.4/31	非オーナー

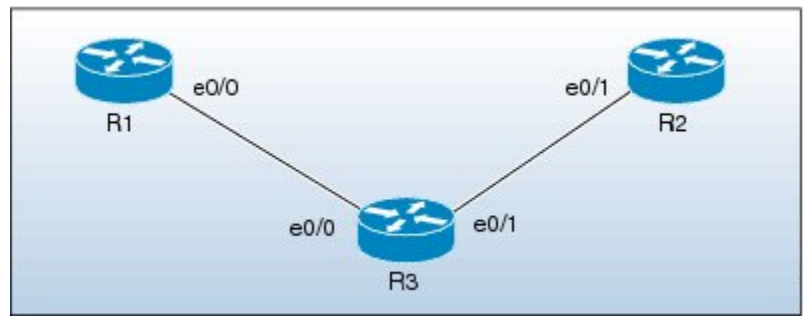
自動 IP リングからのデバイスの削除

既存の自動 IP リングからデバイスを手動で削除できます。



(注) IP リングからデバイスを削除してネイバーデバイスを接続する場合、設定は必要ありません。

下の図のトポロジはシナリオ例を示しています。



このトポロジでは、デバイス R3 が自動 IP リングから削除され、デバイス R1 が R2 に接続されています。その結果、自動 IP タイプ/長さ/値 (TLV) が R1 と R2 の間で交換されます。R1 の e0/0 インターフェイスはプライオリティ 2 の自動 IP TLV を送信し、R2 の e0/1 インターフェイスはプライオリティ 0 の自動 IP TLV を R1 上の e0/0 インターフェイスに送信するため、R1 の e0/0 インターフェイスが R1 と R2 を接続するサブネットのオーナー インターフェイスとして指定されます。R1 は R2 の e0/1 インターフェイスに IP アドレスを割り当て、これがこのサブネット上の非オーナー インターフェイスになります。

自動 IP リングから R3 を削除すると、リング トポロジは次のようになります。



サブネットのオーナーと非オーナーのインターフェイスの IP アドレスを次に示します。

デバイス	インターフェイス	名称
R1	e0/0	オーナー

R2	e0/1	非オーナー
----	------	-------

自動スワップテクニックを使用した競合解決

自動スワップテクニックは自動IPリングへの誤ったデバイスの挿入を原因とする競合を自動的に解決します。

自動IPリングからデバイスを削除する場合、ノードインターフェイス上のオーナーと非オーナーの自動IP設定は保持されます。自動IPリングにデバイスを再挿入できます。

間違ってインターフェイスをスワップした状態でリングにデバイスを挿入すると（これにより、オーナーと非オーナーのインターフェイスが接続されるのではなく、2つのオーナーインターフェイスと2つの非オーナーインターフェイスをそれぞれで接続）、自動IPタイプ/長さ/値（TLV）の送信中に同一のプライオリティ値がインターフェイス間で交換されます。これにより、挿入されたデバイスのインターフェイスのノード間で交換されるプライオリティ値が同順位になり、競合が検出されます。

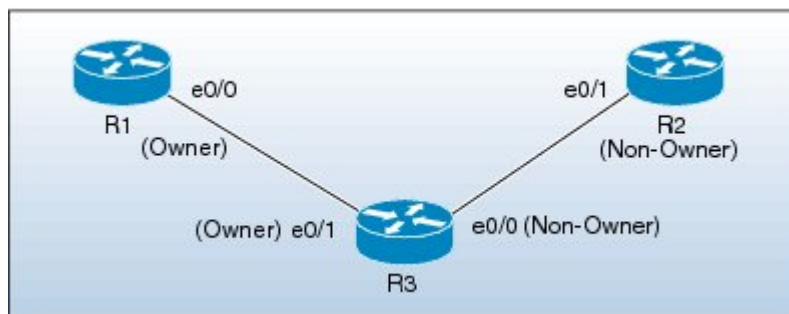
自動スワップテクニックによって、挿入されたデバイスの両ノードインターフェイス上でノードの競合が解決され、インターフェイスに対するIPアドレスの割り当てが可能になります。



(注)

自動スワップテクニックをイネーブルにするために設定は必要ありません。自動的にイネーブルになります。自動スワップテクニックは、デバイスの両方のノードインターフェイス上で競合が検出されているときにのみ使用されます。

下の図のトポロジはシナリオ例を示しています。



このトポロジでは、デバイス R3 がインターフェイスをスワップした正しくない状態でデバイス R1 と R2 の間で挿入されています。次に示すように不適切な挿入が原因で競合が発生します。

- オーナーインターフェイスは別のオーナーインターフェイスに接続されています。つまり、R1 の e0/0 インターフェイスが R3 の e0/1 インターフェイスに接続されています。
- 非オーナーインターフェイスは別の非オーナーインターフェイスに接続されています。つまり、R2 の e0/1 インターフェイスが R3 の e0/0 インターフェイスに接続されています。

R1 と R3 の間の自動 IP TLV 交換の詳細を次に示します。

- R1 上の e0/0 インターフェイスはプライオリティ 2 の自動 IP TLV を R3 上の e0/1 インターフェイスに送信します。
- R3 上の e0/1 インターフェイスはプライオリティ 2 の自動 IP TLV を R1 上の e0/0 インターフェイスに送信します。

同じプライオリティ値 2 が両方のインスタンス内で送信されるため、選択プロセスで同順位があり、競合に至ります。

同様に、R3 の e0/0 インターフェイスおよび R2 の e0/1 インターフェイスは非オーナー インターフェイスであるため、これらの中で同じプライオリティ値 0 が交換されて競合に至ります。

自動スワップ

自動 IP 機能では、挿入されているデバイスの両方のノード インターフェイス上で自動スワップテクニックを使用して競合を解決します。

R3 上の e0/1 インターフェイスのプライオリティおよびインターフェイス IP アドレスが、R3 上の e0/0 インターフェイスのプライオリティおよびインターフェイス IP アドレスとそれぞれスワップされます。

スワップ後、次の自動 IP TLV 情報が R1 と R3 の間で交換されます。

- R1 上の e0/0 インターフェイスはプライオリティ 2 の自動 IP TLV を R3 上の e0/1 インターフェイスに送信します。
- R3 上の e0/1 インターフェイスはプライオリティ 0 の自動 IP TLV を R1 上の e0/0 インターフェイスに送信します。

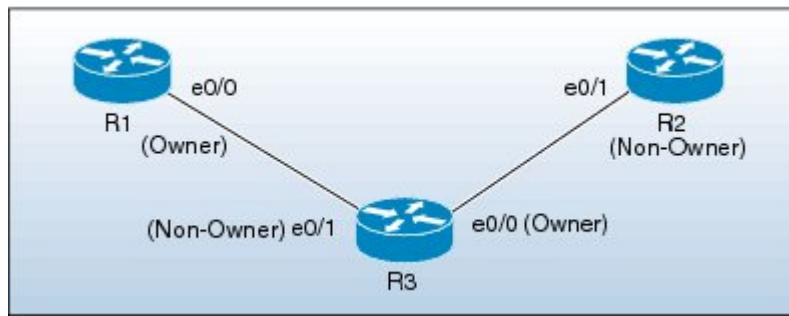
R1 から R3 に送信されたプライオリティは R3 上の e0/1 インターフェイスによって送信されたプライオリティよりも高いため、R3 では R1 (10.1.1.1) の自動 IP アドレスから e0/1 インターフェイス用の IP アドレス 10.1.1.0 を取得します。

次の自動 IP TLV 情報が R3 と R2 の間で交換されます。

- R3 上の e0/0 インターフェイスはプライオリティ 2 の自動 IP TLV を R2 上の e0/1 インターフェイスに送信します。
- R2 上の e0/1 インターフェイスはプライオリティ 0 の自動 IP TLV を R3 上の e0/1 インターフェイスに送信します。

R2 は R3 によって送信されたプライオリティが R2 の e0/1 インターフェイスによって送信されたプライオリティよりも高いことを検出し、R3 (10.1.1.5) の自動 IP アドレスから IP アドレス 10.1.1.4 を取得します。

競合の解決後、トポロジは次のようになります。



R3 上の e0/1 インターフェイスは非オーナー インターフェイスとして指定され、R3 上の e0/0 インターフェイスはオーナー インターフェイスとして指定されています。

自動 IP の設定方法

シード デバイスの設定

自動 IP リング内に少なくとも 1 台のシード デバイスを設定する必要があります。シード デバイスを設定するには、(特定の単一のリングに対して) デバイスの 2 つのノード インターフェイス上に自動 IP アドレスを設定し、同じ IP アドレスを使用して 2 つのノード インターフェイスの 1 つに IP アドレスを設定する必要があります。



注目

Virtual Routing and Forwarding (VRF) インスタンス インターフェイス、スイッチ仮想インターフェイス (SVI)、および EtherChannel 上で自動 IP を設定する前に、次の概念について理解してください。

- VRF : VRF インターフェイス上で自動 IP をイネーブルにする場合は、ノード インターフェイスが現在 VRF 内に存在していることを確認します。インターフェイスが VRF 内に現在存在しない場合は、インターフェイスを VRF に割り当てた後に、VRF インターフェイス上に自動 IP アドレスを設定します。リング用のノード インターフェイスが両方とも同じ VRF に割り当てられていることを確認します。
- SVI : SVI 上の自動 IP 設定は、単一の物理インターフェイスが SVI に関連付けられており、この物理インターフェイスがアクセス ポートであるときだけ可能です。
- EtherChannel : 自動 IP 設定を EtherChannel インターフェイス上で設定することはできませんが、EtherChannel のメンバー インターフェイス上では設定できません。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `lldprun`
4. `interfacetypenumber`
5. `auto-ip-ringring-idipv4-addressauto-ip-address`
6. `exit`
7. `interfacetypenumber`
8. `auto-ip-ringring-idipv4-addressauto-ip-address`
9. `ip addressinterface-ip-address subnet-mask`
10. `end`
11. `showauto-ip-ring [ring-id][detail]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>configureterminal</code> 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	<code>lldprun</code> 例： Device(config)# lldp run	デバイスの Link Layer Discovery Protocol (LLDP) をイネーブルにします。
ステップ 4	<code>interfacetypenumber</code> 例： Device(config)# interface ethernet 0/0	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>auto-ip-ringring-idipv4-addressauto-ip-address</code> 例： Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.1	指定したインターフェイス上の自動 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	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	interfacetype <i>number</i> 例： Device(config)# interface ethernet 0/1	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 8	auto-ip-ring <i>ring-id</i> ipv4-address <i>auto-ip-address</i> 例： Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.1	指定したインターフェイス上の自動 IP アドレスを設定します。
ステップ 9	ip address <i>interface-ip-address subnet-mask</i> 例： Device(config-if)# ip address 10.1.1.1 255.255.255.254	指定したインターフェイス上で IP アドレスを設定します。 (注) 指定したインターフェイスが、シードデバイスのオーナーインターフェイスとして指定されます。
ステップ 10	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 11	show auto-ip-ring [<i>ring-id</i>][detail] 例： Device# show auto-ip-ring 4 detail	自動 IP 情報を表示します。

ノードインターフェイス上における自動 IP 機能の設定（自動 IP リングへの組み込み用）

デバイスを自動 IP リングに挿入するか、既存のリングノード内のインターフェイスをイネーブルにするには、デバイスの 2 個の指定ノードインターフェイス上で自動 IP アドレスを設定する必要があります。



注目 Virtual Routing and Forwarding (VRF) インスタンス インターフェイス、スイッチ仮想インターフェイス (SVI)、および EtherChannel 上で自動 IP を設定する前に、次の概念について理解してください。

- **VRF** : VRF インターフェイス上で自動 IP をイネーブルにする場合は、ノードインターフェイスが現在 VRF 内に存在していることを確認します。インターフェイスが VRF 内に現在存在せず、インターフェイスを VRF 内に配置する必要がある場合は、インターフェイスを VRF 内に移動した後に VRF インターフェイスの上で自動 IP アドレスを設定してください。両方のノードインターフェイスが同じ VRF 内にあることを確認します。
- **SVI** : SVI 上の自動 IP 設定は、単一の物理インターフェイスが SVI に関連付けられており、この物理インターフェイスがアクセスポートであるときだけ可能です。
- **EtherChannel** : 自動 IP 設定を EtherChannel インターフェイス上で設定することはできませんが、EtherChannel のメンバー インターフェイス上では設定できません。

このタスクは、自動 IP リング内の非シードデバイスに適用されます。このタスクを実行する前に、シードデバイスが自動 IP リング用に設定されていることを確認してください。

デバイスの2つのノードインターフェイス上で自動 IP 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `lldprun`
4. `interfacetypenumber`
5. `auto-ip-ringring-idipv4-addressauto-ip-address`
6. `exit`
7. `interfacetypenumber`
8. `auto-ip-ringring-idipv4-addressauto-ip-address`
9. `end`
10. `showauto-ip-ring [ring-id][detail]`

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	configureterminal 例： Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	lldprun 例： Device(config)# lldp run	デバイスの Link Layer Discovery Protocol (LLDP) をイネーブルにします。
ステップ 4	interfacetypenumber 例： Device(config)# interface ethernet 0/1	インターフェイスのタイプおよび番号を指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 5	auto-ip-ringring-idipv4-addressauto-ip-address 例： Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.3	指定したインターフェイス上の自動 IP アドレスを設定します。
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	interfacetypenumber 例： Device(config)# interface ethernet 1/1	インターフェイスのタイプおよび番号を指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 8	auto-ip-ringring-idipv4-addressauto-ip-address 例： Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.3	指定したインターフェイス上の自動 IP アドレスを設定します。
ステップ 9	end 例： Device(config-if)# end	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 auto-ip-ring [<i>ring-id</i>][detail] 例 : Device# show auto-ip-ring 4 detail	自動 IP 情報を表示します。

自動 IP の確認とトラブルシューティング

自動 IP の機能を確認するには、次の作業を実行します。



- (注) これらのコマンドに、特定の順序はありません。**show auto-ip-ring** コマンドは 2 回表示されます。例の 1 つでは、Virtual Routing and Forwarding (VRF) インスタンス インターフェイスの自動 IP リング情報が表示されており、もう 1 つの例では、非 VRF インターフェイスの自動 IP リング情報が表示されています。

手順の概要

1. イネーブル化
2. **show auto-ip-ring** [*ring-id*][**detail**]
3. **show auto-ip-ring** [*ring-id*][**detail**]
4. **debug auto-ip-ring** {*ring-id* {**errors** | **events**} |**errors** | **events**}

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

例 :
Device> **enable**

ステップ 2 **show auto-ip-ring** [*ring-id*][**detail**]

このコマンドは、特定のデバイスまたは自動 IP リングの自動 IP リング情報を表示します。

例 :

Device# **show auto-ip-ring**

Auto-IP ring 1
Auto-IP Address : 10.1.1.5

```

Ring Port0           : Ethernet0/0
My Current-IP       : 0.0.0.0
My Priority          : 1

Auto-IP ring 3
Auto-IP Address     : 10.1.1.3

Ring Port0           : Ethernet0/1
My Current-IP       : 0.0.0.0
My Priority          : 1

```

ステップ3 show auto-ip-ring [ring-id][detail]

このコマンドは、VRF インターフェ이스の自動 IP リング情報を表示します。

例：

```

Device# show auto-ip-ring detail

Auto-IP ring 7
Auto-IP Address     : 10.1.1.11

VRF Name            : 3
Ring Port1          : Ethernet1/1
My Current-IP       : 10.1.1.11
My Priority          : 2

Rx Auto-IP Address  : 10.1.1.13
Rx Current-IP       : 10.1.1.10
Rx Priority          : 0

VRF Name            : 3
Ring Port0          : Ethernet1/0
My Current-IP       : 10.1.1.8
My Priority          : 0

Rx Auto-IP Address  : 10.1.1.9
Rx Current-IP       : 10.1.1.9
Rx Priority          : 2

```

ステップ4 debug auto-ip-ring {ring-id {errors | events} | errors | events}

このコマンドは、指定した自動 IP リングのエラーとイベントをデバッグします。

例：

```

Device# debug auto-ip-ring 1 errors

Auto IP Ring errors debugging is on for the ring id : 1
*Jul 26 11:30:40.541: (Ethernet0/0) priority (value:1) conflict detected, need admin intervention

```

(注) 上記のデバッグ例では、インターフェースから送信されている自動 IP タイプ/長さ/値 (TLV) 内のプライオリティと、ネイバー インターフェースから受信しているプライオリティが同じであるため、競合が検出されています。

自動 IP の設定例

例：シードデバイスの設定

```
Device> enable
Device# configure terminal
Device(config)# lldp run
Device(config)# interface ethernet 0/0
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.1
Device(config-if)# exit
Device(config)# interface ethernet 1/0
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.1
Device(config-if)# ip address 10.1.1.1 255.255.255.254
Device(config-if)# end
```

例：ノードインターフェイス上における自動 IP 機能の設定（自動 IP リングへの組み込み用）

```
Device> enable
Device# configure terminal
Device(config)# lldp run
Device(config)# interface ethernet 0/1
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.3
Device(config-if)# exit
Device(config)# interface ethernet 1/1
Device(config-if)# auto-ip-ring 4 ipv4-address 10.1.1.3
Device(config-if)# end
```

自動 IP に関する追加情報

関連資料

関連項目	マニュアルタイトル
IPv4 アドレスの設定	『IP アドレッシング : IPv4 アドレッシング構成ガイド』
マルチベンダー ネットワークでのリンク レイヤ検出プロトコルの使用	『Carrier Ethernet Configuration Guide』
IPv4 アドレッシング コマンド	『Cisco IOS IP Addressing Services Command Reference』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

シスコのテクニカル サポート

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

自動 IP の機能情報

表 13: 自動 IP の機能情報

機能名	リリース	機能情報
自動 IP	Cisco IOS XE Release 3.10(S)	<p>自動 IP 機能では、自動 IP リング内のノードの挿入、削除、移動に伴うノードの手動再設定の問題に対処します。自動 IP 機能では、自動 IP リングに挿入されたノードインターフェイスに IP アドレスを自動的に提供します。</p> <p>Cisco IOS XE Release 3.10(S) では、Virtual Routing and Forwarding (VRF) インスタンスインターフェイス、SVI、および EtherChannel 上に自動 IP 機能を設定することはできません。</p> <p>次のコマンドが導入または変更されました。 auto-ip-ring、debugauto-ip-ring、showauto-ip-ring。</p>
	Cisco IOS XE Release 3.12(S)	<p>Cisco IOS XE Release 3.12(S) では、Virtual Routing and Forwarding (VRF) インスタンスインターフェイス、SVI、および EtherChannel 上で自動 IP 設定をサポートするように自動 IP 機能が拡張されています。</p> <p>次のコマンドが導入または変更されました。 showauto-ip-ring。</p>



第 6 章

ゼロタッチ自動 IP

ゼロタッチ自動 IP 機能はリングトポロジ内でノードの IP アドレスの自動割り当てと構成を可能にします。IP アドレスは、事前設定した IP アドレスプールから割り当てられます。

自動 IP と比べてゼロタッチ自動 IP には次の利点があります。

- IP アドレスはリングノード上で自動的に設定できます。各ノード上で手動 IP アドレス設定は必要ありません。
- IP アドレスは共通の IP アドレスプールから割り当てられ、IP アドレス範囲を自分で事前定義できます。
- [機能情報の確認](#), 71 ページ
- [ゼロタッチ自動 IP の前提条件](#), 72 ページ
- [ゼロタッチ自動 IP の制約事項](#), 72 ページ
- [ゼロタッチ自動 IP に関する情報](#), 72 ページ
- [ゼロタッチ自動 IP の設定方法](#), 75 ページ
- [ゼロタッチ自動 IP の設定例](#), 84 ページ
- [ゼロタッチ自動 IP に関する追加情報](#), 85 ページ
- [自動 IP の機能情報](#), 86 ページ

機能情報の確認

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

ゼロタッチ自動 IP の前提条件

- Link Layer Discovery Protocol (LLDP) は、すべての自動 IP リングデバイスポート上でイネーブルにする必要があります。
- 自動 IP リングでは、1 台の自動 IP デバイスを自動 IP サーバとして識別する必要があります。
- ゼロタッチ自動 IP リングの一部であると識別されたポートに、自動 IP 機能を手動で設定しないでください。ゼロタッチ自動 IP 設定の対象として識別されているポートに手動による自動 IP 設定がある場合は、そのポートの手動自動 IP 設定をディセーブルにしてください。

ゼロタッチ自動 IP の制約事項

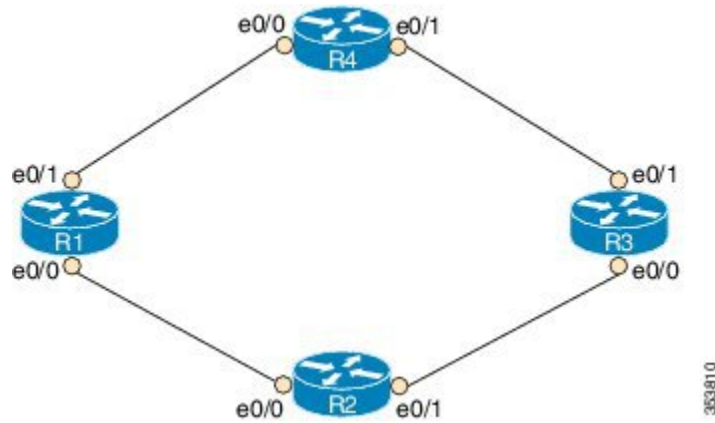
- ゼロタッチ自動 IP と自動 IP は共存できません。ゼロタッチ自動 IP 機能を実装するには、自動 IP リングのすべてのポートは、ゼロタッチ自動 IP ポートとして設定されている必要があります。
- ゼロタッチ自動 IP は指定された自動 IP サーバが自律型ネットワーク内にある場合に機能します。

ゼロタッチ自動 IP に関する情報

ゼロタッチ自動 IP 機能はリングネットワーク内のノード上で IP アドレスを自動設定するという目的を達成するために、自律型ネットワーキングおよび Link Layer Discovery Protocol (LLDP) を使用します。

ゼロタッチ自動 IP 設定のトポロジを検査します。デバイス R1、R2、R3、R4 はリング ネットワークに接続されており、LLDP はすべてのリング ポートでイネーブルになっています。

図 7: ゼロ タッチ自動 IP のトポロジ



ゼロ タッチ自動 IP 機能について知り、設定するには、次に示す情報を使用します。

- 1 リング ネットワーク内の 1 台のデバイス (R1 など) を自律型ネットワークと関連付けます。他の IP デバイスの自律ステータスをイネーブルにします。自律型ネットワークの詳細については、[自律型ネットワーク](#)を参照してください。

```
R1(config)# autonomic registrar
R1(config-registrar)# domain-id auto-addressing.com
R1(config-registrar)# no shutdown
R1(config-registrar)# CA local
R1(config-registrar)# exit
R1(config)# autonomic
```

```
R2(config)# autonomic
R3(config)# autonomic
R4(config)# autonomic
```

R1 はレジストラ上に設定されており、証明書を受け取ることに注意してください。残りのデバイスは自律型デバイスとして設定されています。

- 2 リング内のすべてのポート上で *auto* モードをイネーブルにして自動 IP アドレス設定をイネーブルにします。auto モードは、R1、R2、R3、および R4 の e0/0 ポートと e0/1 ポートでイネーブルにする必要があります。同じデバイスのポートは、リング ID が同一である必要があります。

```
Device(config-if)# auto-ip-ring 1 ipv4-auto
```

- 3 自律型ネットワーク (R1) に追加されたデバイスを自動 IP サーバとして設定します。サーバは IP アドレスのプールを保管します。

```
R1(config)# auto-ip-ring server
```

- 4 自動 IP サーバ上でリング ポートへの IP アドレスの割り当て用に IP アドレスのプールを予約します。



- (注) ゼロタッチおよび手動自動 IP 設定では、オーナーと非オーナーポートのペアに対して /31 の IP サブネットが作成されます（各デバイスがオーナーと非オーナーポートを持つことになる）。偶数番号の IP アドレス（10.1.1.10 など）はオーナーポート用に発行され、奇数番号の IP アドレス（10.1.1.11 など）は非オーナーポート用に予約されます。したがって、自動 IP リングを構成するデバイスの数（または /31 サブネット）とともに、範囲の最初の IP アドレスを指定してください。

```
R1 (config-auto-ip-server) # ipv4-address-pool 10.1.1.10 6
```

この結果、10.1.1.10 から 10.1.1.21 までの IP アドレスの範囲が、自動 IP リング用に割り当てられます。自動 IP サーバが自律型ネットワークに追加され、自律型ネットワーク内の他のノードによって到達可能です。



- (注) 6 台のデバイス用の IP アドレスが予約されることとなります（ただし、要件ではデバイス 4 台）。追加の IP アドレスはリングに新しいデバイスを追加するときに割り当てられます。

- 5 自動 IP ネゴシエーションプロセス：IP アドレスはネゴシエーションプロセスを通じて自動 IP リングノードに割り当てられます。プロセスを開始するには、シードポートとして 1 つのポートを自動 IP リング内で設定します。

```
R1 (config-if) # auto-ip-ring 1 ipv4-seed
```

ネゴシエーションプロセスは次のとおりです。

- 1 シードポートのプライオリティ（R1 上のポートの 1 つなど）は 2 に設定され、これがオーナーポートになります。予約済みプールからの IP アドレスがポートに設定されます。
 - 2 シードポートは接続されたネイバーにシードポートのプライオリティ（2）をアドバタイズし、ネイバーポートを非オーナーにします。シードポートはネイバーポートに IP アドレスを割り当て、ネイバーポートのプライオリティが 0 に変更されます。
 - 3 リング内の各オーナーポートは自動 IP サーバから IP アドレスを取得します。オーナーポートは、接続されたネイバーポートに IP アドレスを割り当てます。
- 6 自動 IP 通信：初期設定後の各オーナーポートは自動 IP サーバに定期的にメッセージを送信して IP アドレスを確保し続けます。オーナーポートから自動 IP サーバに 15 分間メッセージがない場合、サーバは使用可能な IP アドレスのプールに IP アドレスを移動します。

次は、ゼロタッチ自動 IP を設定するコンテキストで、注意すべきポイントの一部です。

- LLDP は自動 IP 設定よりも前にすべての自動 IP リングポートでイネーブルにされている必要があります。
- リングに新しいインターフェイスを挿入する前に、リングポート上で auto モードを設定してください。

- ゼロタッチ自動 IP 設定の場合は、自動 IP リングを構成するデバイス（または /31 サブネット）の数は、1 ～ 128 個である必要があります。
- IP アドレスのプールを指定するときは、指定した範囲内の IP アドレスがすでに使用されていないことを確認してください。
- 後でリングトポロジにデバイスを追加する場合に備えて、自動 IP リング用の追加の IP アドレスを必ず予約してください。
- 自動 IP アドレスプールの予約に使用される開始 IP アドレスは偶数でなければなりません。たとえば、10.1.1.10 は IP アドレスとして有効ですが、10.1.1.9 は無効です。
- 自動 IP リングからデバイスを削除すると、自動 IP アドレスは解放されて自動 IP サーバに返却されます。

ゼロタッチ自動 IP の設定方法

自動 IP サーバと自律型ネットワークの関連付け

自動 IP サーバ (R1) は自律型ネットワークに関連付けられている必要があります。Autonomic Network Registrar 内で設定されている必要があります。ネットワーク内の他のデバイス (R2、R3、R4) は自律ステータスを指定してイネーブルにされている必要があります。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `autonomic registrar`
4. `domain-id auto-addressing.com`
5. `no shutdown`
6. `CA local`
7. `exit`
8. `autonomic`
9. `autonomic`
10. `autonomic`
11. `autonomic`
12. `exit`

手順の詳細

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

	コマンドまたはアクション	目的
	例 : R1> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例 : R1# 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	autonomic registrar 例 : R1(config)# autonomic registrar	Autonomic Network Registrar 内で自動 IP サーバをイネーブルにし、レジストラ 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	domain-id auto-addressing.com 例 : R1(config-registrar)# domain-id auto-addressing.com	レジストラに登録しているすべてのデバイスの共通グループを示します。 (注) R1 を AN Registrar 上で設定すると、R1 は自動 IP リング デバイス R2、R3、および R4 を表します。
ステップ 5	no shutdown 例 : R1(config-registrar)# no shutdown	自律型レジストラをイネーブルにします。
ステップ 6	CA local 例 : R1(config-registrar)# CA local	自動 IP サーバにローカル CA 証明書を発行します。
ステップ 7	exit 例 : R1(config-registrar)# exit	レジストラ コンフィギュレーション モードを終了して、グローバルコンフィギュレーションモードを開始します。
ステップ 8	autonomic 例 : R1(config)# autonomic	自律型デバイスとして自動 IP サーバを設定します。 (注) 以下の手順で示すように、自動 IP リング内の残りのデバイス (R2、R3、R4) を自律型ネットワークと関連付ける必要があります。

	コマンドまたはアクション	目的
ステップ 9	autonomic 例： R2(config)# autonomic	自律型デバイスとして R2 を設定します。
ステップ 10	autonomic 例： R3(config)# autonomic	自律型デバイスとして R3 を設定します。
ステップ 11	autonomic 例： R4(config)# autonomic	自律型デバイスとして R4 を設定します。
ステップ 12	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。

次の作業

自動 IP リング ポート上での auto モードのイネーブル化

自動 IP リング ポート上での auto モードのイネーブル化

はじめる前に

自動 IP リングの一部になるポートを識別します。自動 IP リング内のすべてのポート上で auto モードをイネーブルにする必要があることに留意してください。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `lldprun`
4. `interfacetypenumber`
5. `auto-ip-ringring-idipv4-auto`
6. `exit`
7. 手順を反復して、各自動 IP リング ポート上で auto モードを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	lldprun 例： Device(config)# lldp run	デバイスの Link Layer Discovery Protocol (LLDP) をイネーブルにします。
ステップ 4	interfacetypenumber 例： Device(config)# interface ethernet 0/0	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	auto-ip-ringring-idipv4-auto 例： Device(config-if)# auto-ip-ring 1 ipv4-auto	自動 IP リングポート上で auto モードを設定します。
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	手順を反復して、各自動 IP リングポート上で auto モードを設定します。	---

次の作業

自動 IP サーバを設定し、自動 IP リングポート用に IP アドレス プールを予約します。

自動 IP サーバの設定とサーバ上での IP アドレス プールの予約

はじめる前に

リングのすべてのポートが識別されており、ポートで auto モードがイネーブルになっていることを確認します。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `auto-ip-ring server`
4. `ipv4-address-poolauto-ipv4-addressnumber-of-subnets`
5. `exit`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： 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	<code>configureterminal</code> 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	<code>auto-ip-ring server</code> 例： Device(config)# auto-ip-ring server	デバイスを自動 IP サーバとして設定し、自動 IP サーバ 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	<code>ipv4-address-poolauto-ipv4-addressnumber-of-subnets</code> 例： Device(config-auto-ip-server)# ipv4-address-pool 10.1.1.10 6	自動 IP サーバ上で IP アドレスのプールを予約します。 サブネットの数は、リング内のオーナー ポートまたはデバイスの合計数以上である必要があります。奇数番号の IP アドレスがオーナー ポートに割り当てられ、各非オーナー ポートは LLDP 経由でオーナー ポートから IP アドレスを取得します

	コマンドまたはアクション	目的
ステップ 5	exit 例： Device(config-auto-ip-server)# exit	自動 IP サーバ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。

次の作業

自動 IP ネゴシエーションプロセスを開始するようにシードポートを設定します。

シードポートの設定

はじめる前に

すべての自動 IP ポートが auto モードであり、IP アドレスのプールが自動 IP ポート用に予約済みであることを確認します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacetypenumber**
4. **auto-ip-ringring-idipv4-seed**
5. **exit**
6. **end**
7. **showauto-ip-ring [ring-id][detail]**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	interface <i>type</i> <i>number</i> 例： Device(config)# interface ethernet 0/1	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	auto-ip-ring <i>ring-id</i> ipv4-seed 例： Device(config-if)# auto-ip-ring 1 ipv4-seed	ポートをシードポートとして指定し、自動 IP ネゴシエーションプロセスを開始します。
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	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	show auto-ip-ring [<i>ring-id</i>][detail] 例： Device# show auto-ip-ring 4 detail	自動 IP 情報を表示します。

次の作業

IP アドレスが設定されていることを確認します。

ゼロタッチ自動 IP の確認とトラブルシューティング

ゼロタッチ自動 IP の機能を確認するには、次の作業を実行します。



(注) これらのコマンドに、特定の順序はありません。

手順の概要

1. イネーブル化
2. `show auto-ip-ring [ring-id][detail]`
3. `show autonomic service`
4. `show autonomic device`
5. `show autonomic neighbors`
6. `debug auto-ip-ring {ring-id {errors | events} |errors | events}`

手順の詳細

ステップ1 イネーブル化

特権 EXEC モードをイネーブルにします。

例：

```
Device> enable
```

ステップ2 `show auto-ip-ring [ring-id][detail]`

このコマンドは、特定のデバイスまたは自動 IP リングの自動 IP リング情報を表示します。以下の出力例には、単一のリングを表している 2 個のポート、このポートの IP アドレス、接続先のポートと IP アドレス（ネイバー ポート情報は Rx と表記）が表示されています。

例：

```
Device# show auto-ip-ring 1
Auto-IP ring 1
Auto-IP Address       : 10.1.1.11
Ring Port0            : Ethernet0/1
My Current-IP         : 10.1.1.11
My Priority             : 2
Rx Auto-IP Address    : 10.1.1.13
Rx Current-IP         : 10.1.1.12
Rx-Priority           : 0
Ring Port1            : Ethernet0/0
My Current-IP         : 10.1.1.10
My Priority             : 0
Rx Auto-IP Address    : 10.1.1.17
Rx Current-IP         : 10.1.1.17
Rx-Priority           : 2
```

ステップ3 `show autonomic service`

次に、このコマンドの出力例を示します。自律型ネットワークに接続されたデバイスに設定されている自律サービスが表示されています。

例：

```
Device# show autonomic service

Service                IP-Addr
Autonomic registrar    FD53:EE55:A541:0:AABB:CC00:100:1
ANR type                IOS CA
Auto IP Server          FD53:EE55:A541:0:AABB:CC00:100:1
```

ステップ 4 show autonomic device

次に、このコマンドの出力例を示します。自律型ネットワークに接続されたデバイスの自律型ネットワーク設定クレデンシャルが表示されています。固有識別子 (UDI)、デバイス識別子 (Device ID)、関連付けられたドメイン (Domain ID) などの詳細が表示されています。

例：

```
Device# show autonomic device

UDI                PID:Unix SN:655773698
Device ID          aabb.cc00.0100-2
Domain ID          auto-networking.ID
Domain Certificate (sub:) ou=abcd.com+serialNumber=PID:Unix
SN:655773698,cn=aabb.cc00.0100-2
Certificate Serial Number 03
Device Address     FD53:EE55:A541:0:AABB:CC00:100:2
Domain Cert is Valid
```

ステップ 5 show autonomic neighbors

次に、このコマンドの出力例を示します。接続されたネイバーデバイスの自律設定の詳細が表示されます。固有識別子 (UDI)、デバイス識別子 (Device ID)、関連付けられたドメイン (Domain ID) などの詳細が表示されています。

例：

```
Device# show autonomic neighbors

-----
UDI                Device-ID          Domain          Interface
-----
PID:Unix SN:655773697    aabb.cc00.0100-1    abcd.com
Ethernet0/0
PID:Unix SN:655773699    aabb.cc00.0100-4    abcd.com    Ethernet0/1
```

ステップ 6 debug auto-ip-ring {ring-id {errors | events} | errors | events}

次に、このコマンドの出力例を示します。指定した自動 IP リングのデバッグ エラーおよびイベントが表示されています。

- (注) デバッグ出力例では、インターフェイスから送信されている自動 IP タイプ/長さ/値 (TLV) 内のプライオリティと、ネイバー インターフェイスから受信しているプライオリティが同じであるため、競合が検出されています。

例 :

```
Device# debug auto-ip-ring 2 errors

Auto IP Ring errors debugging is on for the ring id : 2
*Jul 26 11:30:40.541: (Ethernet0/0) priority (value:1) conflict detected, need admin intervention
```

ゼロタッチ自動 IP の設定例

例 : 自動 IP サーバと自律型ネットワークの関連付け

自動 IP サーバ (R1) は自律型ネットワークに関連付けられています。ネットワーク内の他のデバイス (R2、R3、R4) は自律ステータスを指定してイネーブルにされています。

```
R1(config)# autonomous registrar
R1(config-registrar)# domain-id auto-addressing.com
R1(config-registrar)# no shutdown
R1(config-registrar)# CA local
R1(config-registrar)# exit
R1(config)# autonomous
```

```
R2(config)# autonomous
R3(config)# autonomous
R4(config)# autonomous
```

例 : 自動 IP リング ポート上での auto モードのイネーブル化

```
Device> enable
Device# configure terminal
Device(config)# lldp run
Device(config)# interface ethernet 0/0
Device(config-if)# auto-ip-ring 1 ipv4-auto
Device(config-if)# exit
```

Repeat the preceding steps to configure the auto mode on each Auto-IP ring port

例 : 自動 IP サーバの設定とサーバ上での IP アドレス プールの予約

```
Device> enable
Device# configure terminal
```

```
Device(config)# auto-ip-ring server
Device(config-auto-ip-server)# ipv4-address-pool 10.1.1.10 6
Device(config-auto-ip-server)# exit
```

例：シードポートの設定

```
Device> enable
Device# configure terminal
Device(config)# interface e0/0
Device(config-if)# auto-ip-ring 1 ipv4-seed
Device(config-if)# exit
```

ゼロタッチ自動 IP に関する追加情報

関連資料

関連項目	マニュアルタイトル
自動 IP	『IP アドレッシング：IPv4 アドレッシング構成ガイド』
IPv4 アドレスの設定	『IP アドレッシング：IPv4 アドレッシング構成ガイド』
マルチベンダー ネットワークでのリンク レイヤ検出プロトコルの使用	『Carrier Ethernet Configuration Guide』
IPv4 アドレッシング コマンド	『Cisco IOS IP Addressing Services Command Reference』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

シスコのテクニカル サポート

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

自動 IP の機能情報

表 14: 自動 IP の機能情報

機能名	リリース	機能情報
ゼロ タッチ自動 IP	Cisco IOS XE Release 3.15S	<p>ゼロ タッチ自動 IP 機能は自動 IP リング内でノードの IP アドレスの自動割り当てと構成を可能にします。IP アドレスは、IP アドレス プールから割り当てられます。</p> <p>次のコマンドが導入または変更されました。 auto-ip-ring ipv4-auto、auto-ip-ring ipv4-seed、auto-ip-ring server、ipv4-address-pool。</p>