



# 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。

## このモジュール内の機能情報の検索

ご使用の Cisco IOS ソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「[IP アドレスの機能情報](#)」(P.27) を参照してください。

## プラットフォームと、Cisco IOS および Catalyst OS ソフトウェア イメージに関するサポート情報の検索

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。

## 目次

- 「[IP アドレスに関する情報](#)」(P.2)
- 「[IP アドレスの設定方法](#)」(P.11)
- 「[IP アドレスの設定例](#)」(P.22)
- 「[次の作業](#)」(P.24)
- 「[参考資料](#)」(P.24)
- 「[IP アドレスの機能情報](#)」(P.27)



## IP アドレスに関する情報

IP アドレスを設定するには、次の概念を理解しておく必要があります。

- 「2 進数ナンバリング」(P.2)
- 「IP アドレスの構造」(P.4)
- 「IP アドレス クラス」(P.5)
- 「IP ネットワークのサブネット化」(P.7)
- 「IP ネットワーク アドレス割り当て」(P.8)
- 「クラスレス Inter-Domain ルーティング」(P.11)
- 「プレフィクス」(P.11)

## 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と、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。図 1 に、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
= 255

186266

図 2 に、0 ～ 255 における 2 進数から 10 進数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

186267

図 3 に、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	

186271

## 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。

表 1 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
192.168.100.4	11000000.10101000.01100100.00000100



(注)

表 1 の IP アドレスは、RFC 1918『*Address Allocation for Private Internets*』のもので、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。

表 2 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)	<b>0.0.0.0</b> ~ 127.0.0.0/8 (255.0.0.0)
A (2 進数形式の範囲)	<b>00000000.00000000.00000000.00000000</b> ~ <b>01111111.00000000.00000000.00000000</b>
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)	<b>128.0.0.0</b> ~ <b>191.255.0.0</b> /16 (255.255.0.0)
B (2 進数形式の範囲)	<b>10000000.00000000.00000000.00000000</b> ~ <b>10111111.11111111.00000000.00000000</b>
B (2 進数形式のマスク)	11111111.11111111.00000000.00000000/16
C (ドット付き 10 進形式の範囲/マスク)	<b>192.0.0.0</b> ~ <b>223.255.255.0</b> /24 (255.255.255.0)
C (2 進数形式の範囲)	<b>11000000.00000000.00000000.00000000</b> ~ <b>11011111.11111111.11111111.00000000</b>
C (2 進数形式のマスク)	11111111.11111111.11111111.00000000/24
D <sup>1</sup> (ドット付き 10 進形式の範囲/マスク)	<b>224.0.0.0</b> ~ <b>239.255.255.255</b> /32 (255.255.255.255)
D (2 進数形式の範囲)	<b>11100000.00000000.00000000.00000000</b> ~ <b>11101111.11111111.11111111.11111111</b>
D (2 進数形式のマスク)	11111111.11111111.11111111.11111111/32
E <sup>2</sup> (ドット付き 10 進形式の範囲/マスク)	<b>240.0.0.0</b> ~ <b>255.255.255.255</b> /32 (255.255.255.255)

表 2 クラスおよびマスク別の IP アドレス範囲 (続き)

クラス	範囲
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。各クラスで使用できる IP ネットワーク アドレスの範囲は、使用できるビットの数で 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 (表 2) 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 で使用できる IP ネットワーク アドレスは 128 あります ( $2^7 = 128$ )。

IP アドレス クラスで使用できる IP ホスト アドレスの数は、使用できるビットの数で 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 アドレスで使用できるビットは 24 あります。そのため、クラス A で使用できる IP ホスト アドレスは 16,777,214 あります ( $(2^{24}) - 2 = 16,777,214$ )。



(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。

表 3 に、各クラスの IP アドレスで使用できる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 アドレスで使用できる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 <sup>1</sup>	65534
C	2,097,152 <sup>2</sup>	254

1. 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 アドレスで使用できるビットは 14 だけです。

- 表 2 に示すように、最初の 3 ビットは常に 110 になるため、クラス C の IP ネットワーク アドレスで使用できるビットは 21 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 ( $16 \times 65,534 = 1,048,544$ ) です。単一のネットワーク セグメントで 65,534 のホストを使用できるネットワーク 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性がありました。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 のサブネット IP アドレスを使用できます ( $2^4 = 16$ )。表 4 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

数値	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 <sup>1</sup>	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

- 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 172.48.121.34/20 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 ルートのアドバイタズ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できるすべての 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 レイヤ（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。

図 4 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 のルーティング テーブルは、表 5 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

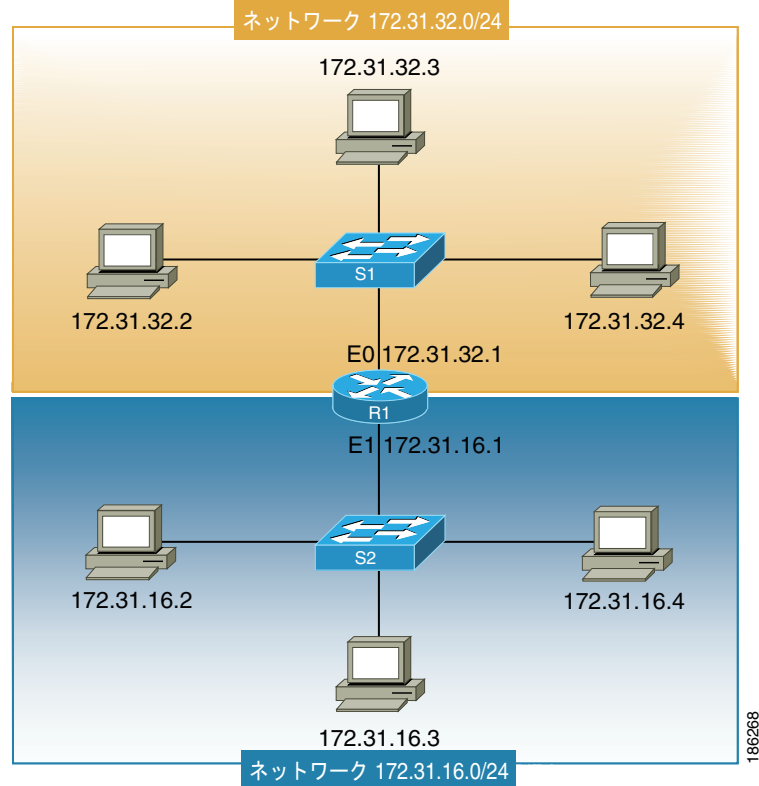


図 5 に、IP ネットワーク アドレスが正しく設定されていない簡単なネットワークの例を示します。R1 のルーティング テーブルは、表 6 のようになります。IP アドレスが 172.31.32.3 の PC が、IP アドレス 172.31.32.54 の PC に IP トラフィックを送信しようとした場合、ルータ R1 は、IP アドレスが 172.31.32.54 の PC の接続先となるインターフェイスを判別できません。

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)

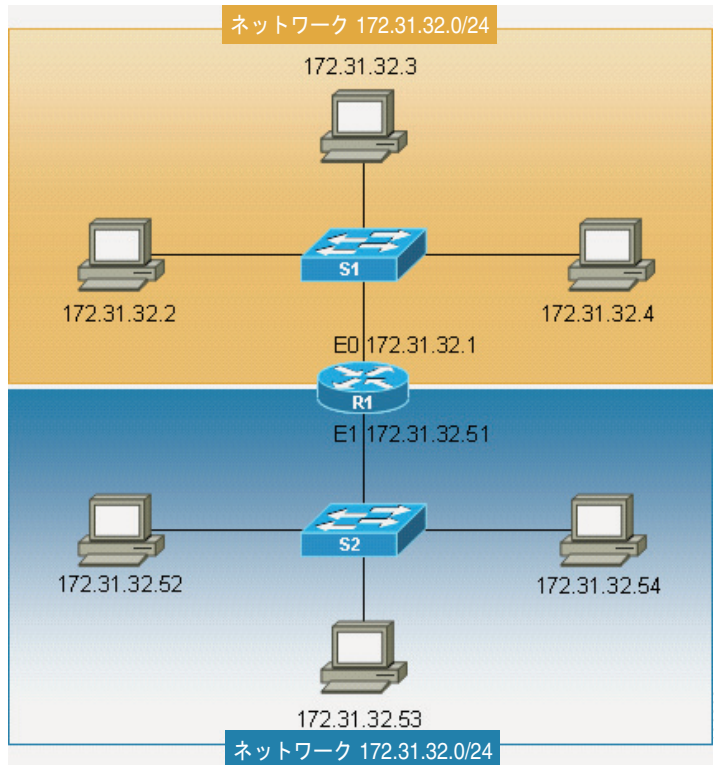


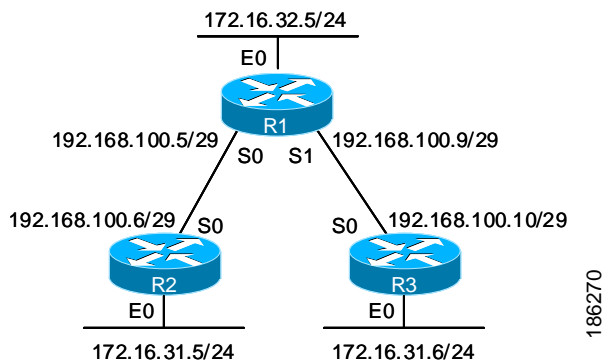
図 5 のような間違いを防止するため、Cisco IOS-based ネットワーキング デバイスでは、IP ルーティングがイネーブルにされている場合にルータの複数のインターフェイスで同じ IP ネットワーク アドレスを設定できません。

172.16.31.0/24 が R2 および R3 で使用されている、図 6 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) 172.16.31.0/24 RIP	192.168.100.8/29 (接続) 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](#)」(P.25) 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。

## クラスレス Inter-Domain ルーティング

インターネットの使用が増加を続け、表 2 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。

## プレフィクス

プレフィクスという用語は、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 ビットのプレフィクスを使用するということができます。

CIDR を使用する場合、プレフィクスは、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

ここでは、次の作業について説明します。

- 「[IP アドレスをインターフェイスに割り当てることによるネットワークとの IP 接続の確立](#)」(P.11)
- 「[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](#)」(P.13)
- 「[ポイントツーポイント WAN インターフェイスでの IP アンナナンバーを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減](#)」(P.14)
- 「[ポイントツーポイント WAN インターフェイスで 31 ビットプレフィクスの IP アドレスを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減](#)」(P.16)
- 「[IP サブネットゼロの使用を許可することによる、使用できる IP サブネットの数の最大化](#)」(P.19)
- 「[ネットワークマスクの形式の指定](#)」(P.20)

## IP アドレスをインターフェイスに割り当てることによ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. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shutdown**
5. **ip address** *ip-address mask*
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	<b>enable</b>  例： Router> 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	<b>configure terminal</b>  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	<b>interface</b> <i>type number</i>  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	<b>no shutdown</b>  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	<b>ip address</b> <i>ip-address mask</i>  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	<b>end</b>  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。

## 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できる 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、セカンダリ 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. **enable**
2. **configure terminal**
3. **interface type number**
4. **no shutdown**
5. **ip address ip-address mask**
6. **ip address ip-address mask secondary**
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	<b>enable</b>  例： Router> 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	<b>configure terminal</b>  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	<b>interface type number</b>  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	<b>no shutdown</b>  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	<b>ip address ip-address mask</b>  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。

	コマンドまたはアクション	目的
ステップ 6	<pre>ip address ip-address mask secondary</pre> <p>例:</p> <pre>Router(config-if)# ip address 172.16.32.1 255.255.240.0 secondary</pre>	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。
ステップ 7	<pre>end</pre> <p>例:</p> <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。

- **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。

## 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ダプ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、次の URL の『[Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T](http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/12_4t/irp_12_4t_book.html)』を参照してください。

[http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/12\\_4t/irp\\_12\\_4t\\_book.html](http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/12_4t/irp_12_4t_book.html).

## ポイントツーポイント WAN インターフェイスでの IP アンナンバードを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減

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」 (P.15)
- 「制約事項」 (P.15)
- 「手順の概要」 (P.15)
- 「手順の詳細」 (P.15)
- 「トラブルシューティングのヒント」 (P.16)

## 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。

## 制約事項

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. **enable**
2. **configure terminal**
3. **interface type number**
4. **no shutdown**
5. **ip address ip-address mask**
6. **interface type number**
7. **no shutdown**
8. **ip unnumbered type number**
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	<b>enable</b>  例： Router> 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	<b>configure terminal</b>  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	<b>interface type number</b>  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。

	コマンドまたはアクション	目的
ステップ 4	<code>no shutdown</code>  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	<code>ip address ip-address mask</code>  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	<code>interface type number</code>  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	<code>no shutdown</code>  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。
ステップ 8	<code>ip unnumbered type number</code>  例： Router(config-if)# ip unnumbered fastethernet 0/0	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	<code>end</code>  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。

## ポイントツーポイント WAN インターフェイスで 31 ビット プレフィクスの IP アドレスを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減

ネットワーキング デバイスにより使用される IP サブネットの数を削減して、RFC 3021 で規定されている 31 ビット プレフィクスの 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」\(P.17\)](#)



- 「前提条件」 (P.18)
- 「制約事項」 (P.18)
- 「手順の概要」 (P.18)
- 「手順の詳細」 (P.18)
- 「トラブルシューティングのヒント」 (P.19)

## 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)、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。

表 8 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

Address	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 <b>100</b>
192.168.100.5/30	最初のホストアドレス	11000000.10101000.01100100.00000 <b>101</b>
192.168.100.6/30	2 番めのホストアドレス	11000000.10101000.01100100.00000 <b>110</b>
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 <b>111</b>

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 packets 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。RFC 3021 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。

表 9 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

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

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。

## 前提条件

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 **ip classless** 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。

## 制約事項

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. **enable**
2. **configure terminal**
3. **ip classless**
4. **interface *type number***
5. **no shutdown**
6. **ip address *ip-address mask***
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	<b>enable</b>  例： Router> 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	<b>configure terminal</b>  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	<b>ip classless</b>  例： Router(config)# ip classless	(任意) IP クラスレス (CIDR) をイネーブルにします。  (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 <b>ip classless</b> 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。 <b>ip classless</b> 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。

	コマンドまたはアクション	目的
ステップ 4	<code>interface type number</code>  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	<code>no shutdown</code>  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	<code>ip address ip-address mask</code>  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	<code>end</code>  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 サブネット ゼロの使用を許可することによる、使用できる IP サブネットの数の最大化

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できるネットワーク アドレスが 1 つ追加されます。表 4 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. **enable**
2. **configure terminal**
3. **ip subnet-zero**
4. **interface type number**
5. **no shutdown**
6. **ip address ip-address mask**
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	<code>enable</code>  例： Router> 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	<code>configure terminal</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>ip subnet-zero</code>  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	<code>interface type number</code>  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	<code>no shutdown</code>  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	<code>ip address ip-address mask</code>  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	<code>end</code>  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。

## ネットワーク マスクの形式の指定

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 (/) とネットワーク 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 として表示されます。

- 「現在のセッションでのネットマスクの表示形式の指定」
- 「個々の回線でのネットマスクの表示形式の指定」

## 現在のセッションでのネットマスクの表示形式の指定

現在のセッションでのネットマスクの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. `enable`
2. `term ip netmask-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	<code>enable</code>  例： Router> 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	<code>term ip netmask-format {bitcount   decimal   hexadecimal}</code>  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。

## 個々の回線でのネットマスクの表示形式の指定

個々の回線でのネットマスクの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. `enable`
2. `configure terminal`
3. `line vty first last`
4. `term ip netmask-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	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<code>configure terminal</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>line vty first last</code>  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	<code>term ip netmask-format {bitcount   decimal   hexadecimal}</code>  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	<code>end</code>  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。

## IP アドレスの設定例

ここでは、次の設定例について説明します。

- 「IP アドレスをインターフェイスに割り当てることによるネットワークとの IP 接続の確立：例」(P.22)
- 「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：例」(P.23)
- 「ポイントツーポイント WAN インターフェイスでの IP アナンバードを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減：例」(P.23)
- 「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 アドレスを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減：例」(P.24)
- 「IP サブネット ゼロの使用を許可することによる、使用できる IP サブネットの数の最大化：例」(P.24)

## IP アドレスをインターフェイスに割り当てることによるネットワークとの IP 接続の確立：例

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
  !
```

## 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：例

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
  !
```

## ポイントツーポイント WAN インターフェイスでの IP アンナンバードを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減：例

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
!
```

## 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 アドレスを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減：例

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
```

## IP サブネット ゼロの使用を許可することによる、使用できる IP サブネットの数の最大化：例

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、次の URL の『[Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T](http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/12_4t/irp_12_4t_book.html)』を参照してください。

[http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/12\\_4t/irp\\_12\\_4t\\_book.html](http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/12_4t/irp_12_4t_book.html)

## 参考資料

ここでは、IP アドレス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	参照先
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』

## 規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

## MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	—

## RFC

RFC <sup>1</sup>	タイトル
RFC 791	『Internet Protocol』 <a href="http://www.ietf.org/rfc/rfc0791.txt">http://www.ietf.org/rfc/rfc0791.txt</a>
RFC 1338	『Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy』 <a href="http://www.ietf.org/rfc/rfc1519.txt">http://www.ietf.org/rfc/rfc1519.txt</a>
RFC 1466	『Guidelines for Management of IP Address Space』 <a href="http://www.ietf.org/rfc/rfc1466.txt">http://www.ietf.org/rfc/rfc1466.txt</a>
RFC 1716	『Towards Requirements for IP Routers』 <a href="http://www.ietf.org/rfc/rfc1716.txt">http://www.ietf.org/rfc/rfc1716.txt</a>
RFC 1918	『Address Allocation for Private Internets』 <a href="http://www.ietf.org/rfc/rfc1918.txt">http://www.ietf.org/rfc/rfc1918.txt</a>
RFC 3330	『Special-Use IP Addresses』 <a href="http://www.ietf.org/rfc/rfc3330.txt">http://www.ietf.org/rfc/rfc3330.txt</a>

1. 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できる多くの 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
<p>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。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"><li>• テクニカル サポートを受ける</li><li>• ソフトウェアをダウンロードする</li><li>• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける</li><li>• ツールおよびリソースへアクセスする<ul style="list-style-type: none"><li>– Product Alert の受信登録</li><li>– Field Notice の受信登録</li><li>– Bug Toolkit を使用した既知の問題の検索</li></ul></li><li>• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する</li><li>• トレーニング リソースへアクセスする</li><li>• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する</li></ul> <p>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。</p>	<p><a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a></p>

## IP アドレスの機能情報

表 10 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンドリファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。



(注) 表 10 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 10 IP アドレスの機能情報

機能名	リリース	機能情報
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。  次のセクションで、この機能に関する情報を参照できます。 <ul style="list-style-type: none"> <li>「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 アドレスを使用することによる、IP 接続の確立を必要とする IP アドレス数の削減」(P.16)</li> </ul>
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。 <b>ip unnumbered.</b>

表 10 IP アドレスの機能情報 (続き)

機能名	リリース	機能情報
IP サブネット ゼロ	10.0	<p>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。</p> <p>次のコマンドが導入または変更されました。 <b>ip subnet-zero。</b></p>
クラスレス Inter-Domain ルーティング	10.0	<p>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。</p> <p>次のコマンドが導入または変更されました。<b>ip classless。</b></p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](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. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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。

© 2007 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2007–2011, シスコシステムズ合同会社.  
All rights reserved.