IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS XE Release 2

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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: 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)

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

© 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

Configuring IPv4 Addresses

This chapter contains information about and instructions for configuring IPv4 addresses on interfaces that are part of a networking device.

Note All further references to IPv4 addresses in this document use only IP in the text, not IPv4.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

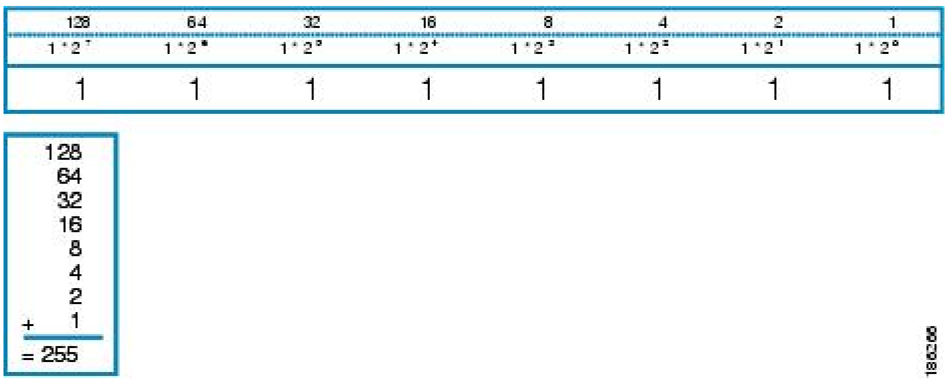
Information About IP Addresses

Binary Numbering

IP addresses are 32 bits long. The 32 bits are divided into four octets (8-bits). A basic understanding of binary numbering is very helpful if you are going to manage IP addresses in a network because changes in the values of the 32 bits indicate either a different IP network address or IP host address.

A value in binary is represented by the number (0 or 1) in each position multiplied by the number 2 to the power of the position of the number in sequence, starting with 0 and increasing to 7, working right to left. The figure below is an example of an 8-digit binary number.

Figure 1 Example of an 8-digit Binary Number



The figure below provides binary to decimal number conversion for 0 through 255.

Figure 2 Binary to Decimal Number Conversion for 0 to 134

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

The figure below provides binary to decimal number conversion for 135 through 255.

Figure 3 Binary to Decimal Number Conversion for 135 to 255

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 Address Structure

An IP host address identifies a device to which IP packets can be sent. An IP network address identifies a specific network segment to which one or more hosts can be connected. The following are characteristics of IP addresses:

- IP addresses are 32 bits long
- IP addresses are divided into four sections of one byte (octet) each
- IP addresses are typically written in a format known as dotted decimal

The table below shows some examples of IP addresses.

Table 1 Examples of IP Addresses

IP Addresses in Dotted Decimal	IP Addresses in Binary
10.34.216.75	00001010.00100010.11011000.01001011
172.16.89.34	10101100.00010000.01011001.00100010
192.168.100.4	11000000.10101000.01100100.00000100

Note The IP addresses in the table above are from RFC 1918, *Address Allocation for Private Internets* . These IP addresses are not routable on the Internet. They are intended for use in private networks. For more information on RFC1918, see http://www.ietf.org/rfc/rfc1918.txt .

IP addresses are further subdivided into two sections known as network and host. The division is accomplished by arbitrarily ranges of IP addresses to classes. For more information see RFC 791 Internet Protocol at http://www.ietf.org/rfc/rfc0791.txt .

IP Address Classes

In order to provide some structure to the way IP addresses are assigned, IP addresses are grouped into classes. Each class has a range of IP addresses. The range of IP addresses in each class is determined by the number of bits allocated to the network section of the 32-bit IP address. The number of bits allocated to the network section is represented by a mask written in dotted decimal or with the abbreviation /*n* where *n* = the numbers of bits in the mask.

The table below lists ranges of IP addresses by class and the masks associated with each class. The digits in bold indicate the network section of the IP address for each class. The remaining digits are available for host IP addresses. For example, IP address 10.90.45.1 with a mask of 255.0.0.0 is broken down into a network IP address of 10.0.0.0 and a host IP address of 0.90.45.1.

Table 2 IP Address Ranges by Class with Masks

Class	Range
A (range/mask in dotted decimal)	**0** .0.0.0 to 127.0.0.0/8 (255.0.0.0)
A (range in binary)	**00000000** .00000000.00000000.00000000 to**01111111**.00000000.00000000.00000000
A (mask in binary)	11111111.00000000.00000000.00000000/8
B (range/mask in dotted decimal)	**128** .0.0.0 to **191.255**.0.0/16 (255.255.0.0)
B (range in binary)	**10000000 .00000000**.00000000.00000000 to**10111111.11111111**.00000000.00000000
B (mask in binary)	**11111111 .11111111**.00000000.00000000/16
C (range/mask in dotted decimal)	**192 .0.0**.0 to **223.255.255**.0/24 (255.255.255.0)
C (range in binary)	**11000000 .00000000.00000000**.00000000 to**11011111.11111111.11111111**.00000000
C (mask in binary)	11111111.11111111.11111111.0000000/24
D[1] (range/mask in dotted decimal)	**224 .0.0.0** to **239.255.255.255**/32 (255.255.255.255)

1 Class D IP addresses are reserved for multicast applications.

Class	Range
D (range in binary)	**11100000 .00000000.00000000.00000000** to**11101111.11111111.11111111.11111111**
D (mask in binary)	11111111.11111111.11111111.11111111/32
E[2] (range/mask in dotted decimal)	**240 .0.0.0** to **255.255.255.255**/32 (255.255.255.255)
E (range in binary)	**11110000 .00000000.00000000.00000000** to**11111111.11111111.11111111.11111111**
E (mask in binary)	11111111.11111111.11111111.11111111/32

Note Some IP addresses in these ranges are reserved for special uses. For more information refer to RFC 3330, *Special-Use IP Addresses* , at http://www.ietf.org/rfc/rfc3330.txt .

When a digit that falls within the network mask changes from 1 to 0 or 0 to 1 the network address is changed. For example, if you change 10101100.00010000.01011001.00100010/16 to 10101100.00110000.01011001.00100010/16 you have changed the network address from 172.16.89.34/16 to 172.48.89.34/16.

When a digit that falls outside the network mask changes from 1 to 0 or 0 to 1 the host address is changed. For example, if you change 10101100.00010000.01011001.00100010/16 to 10101100.00010000.01011001.00100011/16 you have changed the host address from 172.16.89.34/16 to 172.16.89.35/16.

Each class of IP address supports a specific range of IP network addresses and IP host addresses. The range of IP network addresses available for each class is determined with the formula 2 to the power of the number of available bits. In the case of class A addresses, the value of the first bit in the 1st octet (as shown in the table above) is fixed at 0. This leaves 7 bits for creating additional network addresses. Therefore there are 128 IP network addresses available for class A (27 = 128).

The number of IP host addresses available for an IP address class is determined by the formula 2 to the power of the number of available bits minus 2. There are 24 bits available in a class A addresses for IP host addresses. Therefore there are 16,777,214 IP hosts addresses available for class A ((224) - 2 = 16,777,214)).

Note The 2 is subtracted because there are 2 IP addresses that cannot be used for a host. The all 0's host address cannot be used because it is the same as the network address. For example, 10.0.0.0 cannot be both a IP network address and an IP host address. The all 1's address is a broadcast address that is used to reach all hosts on the network. For example, an IP datagram addressed to 10.255.255.255 will be accepted by every host on network 10.0.0.0.

The table below shows the network and host addresses available for each class of IP address.

2 Class E IP addresses are reserved for broadcast traffic.

Table 3 Network and Host Addresses Available for Each Class of IP Address

Class	Network Addresses	Host Addresses
A	128	16,777,214
B	16,384[3]	65534
C	2,097,152[4]	254

IP Network Subnetting

The arbitrary subdivision of network and host bits in IP address classes resulted in an inefficient allocation of IP space. For example, if your network has 16 separate physical segments you will need 16 IP network addresses. If you use 16 class B IP network addresses, you would be able to support 65,534 hosts on each of the physical segments. Your total number of supported host IP addresses is 1,048,544 (16 * 65,534 = 1,048,544). Very few network technologies can scale to having 65,534 hosts on a single network segment. Very few companies need 1,048,544 IP host addresses. This problem required the development of a new strategy that permitted the subdivision of IP network addresses into smaller groupings of IP subnetwork addresses. This strategy is known as subnetting.

If your network has 16 separate physical segments you will need 16 IP subnetwork addresses. This can be accomplished with one class B IP address. For example, start with the class B IP address of 172.16.0.0 you can reserve 4 bits from the third octet as subnet bits. This gives you 16 subnet IP addresses 24 = 16. The table below shows the IP subnets for 172.16.0.0/20.

Table 4 Examples of IP Subnet Addresses using 172.16.0.0/20

Number	IP Subnet Addresses in Dotted Decimal	IP Subnet Addresses in Binary
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

3 There are only 14 bits available for class B IP network addresses because the first 2 bits are fixed at 10 as shown in Table 2 .

4 There are only 21 bits available for class C IP network addresses because the first 3bits are fixed at 110 as shown in Table 2 .

5 The first subnet that has all of the subnet bits set to 0 is referred to as subnet 0 . It is indistinguishable from the network address and must be used carefully.

Number	IP Subnet Addresses in Dotted Decimal	IP Subnet Addresses in Binary
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

When a digit that falls within the subnetwork (subnet) mask changes from 1 to 0 or 0 to 1 the subnetwork address is changed. For example, if you change 10101100.00010000.01011001.00100010/20 to 10101100.00010000.01111001.00100010/20 you have changed the network address from 172.16.89.34/20 to 172.48.121.34/20.

When a digit that falls outside the subnet mask changes from 1 to 0 or 0 to 1 the host address is changed. For example, if you change 10101100.00010000.01011001.00100010/20 to 10101100.00010000.01011001.00100011/20 you have changed the host address from 172.16.89.34/20 to 172.16.89.35/20.

Timesaver To avoid having to do manual IP network, subnetwork, and host calculations, use one of the free IP subnet calculators available on the Internet.

Some people get confused about the terms network address and subnet or subnetwork addresses and when to use them. In the most general sense the term network address means “the IP address that routers use to route traffic to a specific network segment so that the intended destination IP host on that segment can receive it”. Therefore the term network address can apply to both non-subnetted and subnetted IP network addresses. When you are troubleshooting problems with forwarding traffic from a router to a specific IP network address that is actually a subnetted network address, it can help to be more specific by referring to the destination network address as a subnet network address because some routing protocols handle advertising subnet network routes differently from network routes. For example, the default behavior for RIP v2 is to automatically summarize the subnet network addresses that it is connected to their non-subnetted network addresses (172.16.32.0/24 is advertised by RIP v2 as 172.16.0.0/16) when sending routing updates to other routers. Therefore the other routers might have knowledge of the IP network addresses in the network, but not the subnetted network addresses of the IP network addresses.

Tip The term IP address space is sometimes used to refer to a range of IP addresses. For example, "We have to allocate a new IP network address to our network because we have used all of the available IP addresses in the current IP address space".

IP Network Address Assignments

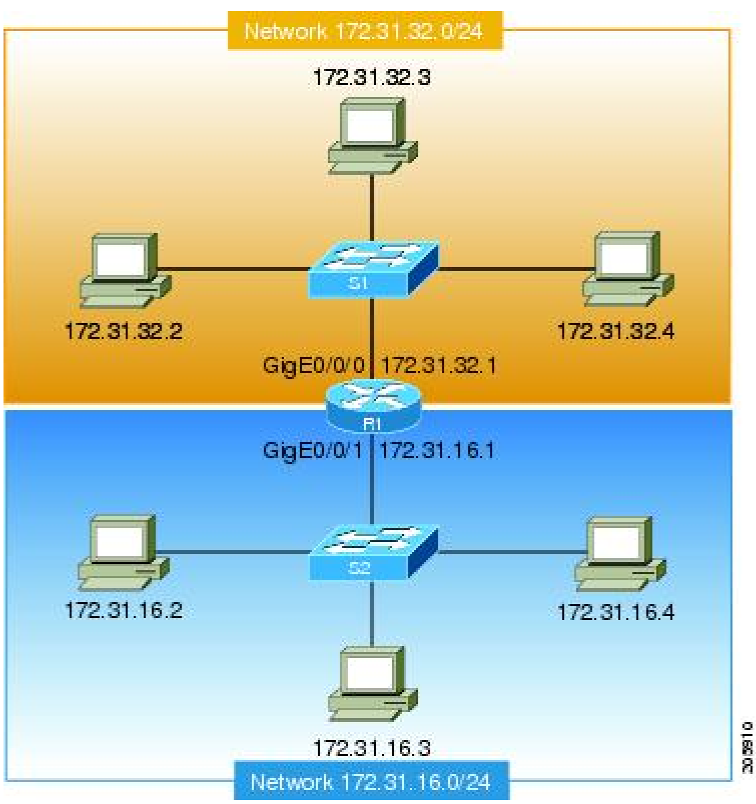
Routers keep track of IP network addresses to understand the network IP topology (layer 3 of the OSI reference model) of the network to ensure that IP traffic can be routed properly. In order for the routers to understand the network layer (IP) topology, every individual physical network segment that is separated from any other physical network segment by a router must have a unique IP network address.

The figure below shows an example of a simple network with correctly configured IP network addresses. The routing table in R1 looks like the table below.

Table 5 Routing Table for a Correctly Configured Network

Interface GigabitEthernet 0/0/0	Interface GigabitEthernet 0/0/1
172.31.32.0/24 (Connected)	172.31.16.0/24 (Connected)

Figure 4 Correctly Configured Network

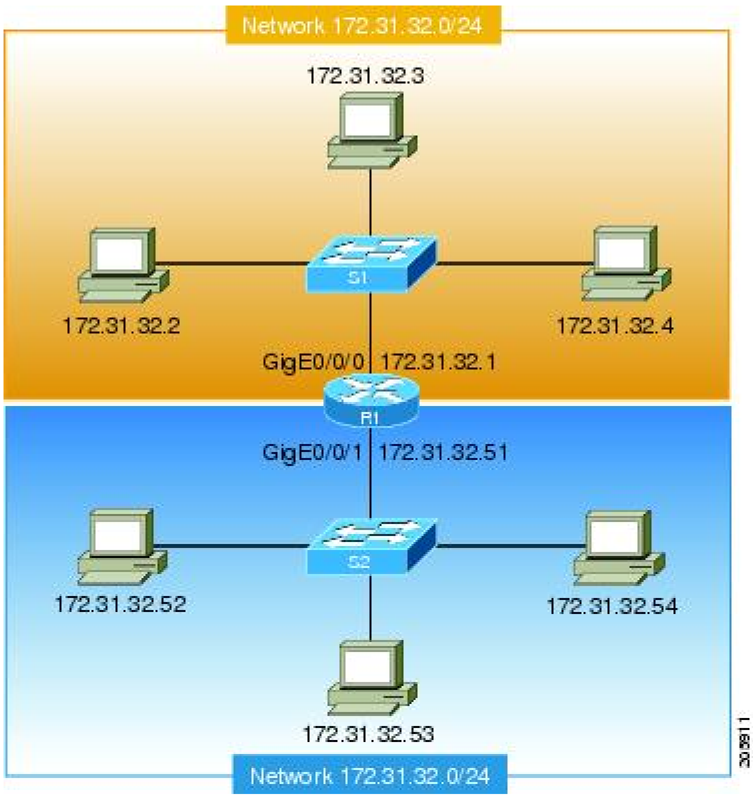


The figure below shows an example of a simple network with incorrectly configured IP network addresses. The routing table in R1 looks like the table below. If the PC with IP address 172.31.32.3 attempts to send IP traffic to the PC with IP address 172.31.32.54, router R1 cannot determine which interface that the PC with IP address 172.31.32.54 is connected to.

Table 6 Routing Table in Router R1 for an Incorrectly Configured Network (Example 1)

GigabitEthernet 0/0/0	GigabitEthernet 0/0/1
172.31.32.0/24 (Connected)	172.31.32.0/24 (Connected)

Figure 5 Incorrectly Configured Network (Example 1)



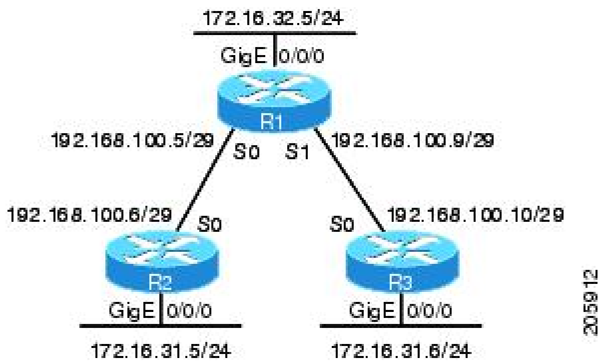
To help prevent mistakes as shown in the figure above, Cisco IOS XE-based networking devices will not allow you to configure the same IP network address on two or more interfaces in the router when IP routing is enabled.

The only way to prevent the mistake shown in the figure below, where 172.16.31.0/24 is used in R2 and R3, is to have very accurate network documentation that shows where you have assigned IP network addresses.

Table 7 Routing Table in Router R1 for an Incorrectly Configured Network (Example 2)

GigabitEthernet 0/0/0	Serial 0	Serial 1
172.16.32.0/24 (Connected)	192.168.100.4/29 (Connected) 172.16.31.0/24 RIP	192.168.100.8/29 (Connected) 172.16.31.0/24 RIP

Figure 6 Incorrectly Configured Network (example 2)



For a more thorough explanation of IP routing, see the "Related Documents" section for a list of documents related to IP routing.

Classless Inter-Domain Routing

Due to the continuing increase in internet use and the limitations on how IP addresses can be assigned using the class structure shown in the table above, a more flexible method for allocating IP addresses was required. The new method is documented in RFC 1519 *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*. CIDR allows network administrators to apply arbitrary masks to IP addresses to create an IP addressing plan that meets the requirements of the networks that they administrate.

For more information on CIDR, refer to RFC 1519 at http://www.ietf.org/rfc/rfc1519.txt.

Prefixes

The term prefix is often used to refer to the number of bits of an IP network address that are of importance for building routing tables. If you are using only classful (strict adherence to A, B, and C network address boundaries) IP addresses, the prefixes are the same as the masks for the classes of addresses. For example, using classful IP addressing, a class C IP network address such as 192.168.10.0 uses a 24-bit mask (/24 or 255.255.255.0) and can also be said to have a 24-bit prefix.

If you are using CIDR, the prefixes are arbitrarily assigned to IP network addresses based on how you want to populate the routing tables in your network. For example, a group of class C IP addresses such as 192.168.10.0, 192.168.11.0, 192.168.12.0, 192.168.13.0 can be advertised as a single route to 192.168.0.0 with a 16-bit prefix (192.168.0.0/16). This results in a 4:1 reduction in the number of routes that the routers in your network need to manage.

How to Configure IP Addresses

Establishing IP Connectivity to a Network by Assigning an IP Address to an Interface

Perform this task to configure an IP address on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shutdown**
5. **ip address** *ip-address mask*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.16.16.1 255.255.240.0`	Configures the IP address on the interface.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 12

Troubleshooting Tips

The following commands can help troubleshoot IP addressing:

- **show ip interface** --Displays the IP parameters for the interface.
- **show ip route connected** --Displays the IP networks the networking device is connected to.

Increasing the Number of IP Hosts that Are Supported on a Network by Using Secondary IP Addresses

If you have a situation in which you need to connect more IP hosts to a network segment and you have used all of the available IP host addresses for the subnet to which you have assigned the segment, you can avoid having to readdress all of the hosts with a different subnet by adding a second IP network address to the network segment.

Perform this task to configure a secondary IP address on an interface.

SUMMARY STEPS

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.16.16.1 255.255.240.0`	Configures the IP address on the interface.

	Command or Action	Purpose
Step 6	**ip address** *ip-address mask* **secondary** **Example:** `Router(config-if)# ip address 172.16.32.1 255.255.240.0 secondary`	Configures the secondary IP address on the interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

- Troubleshooting Tips, page 12
- What to Do Next, page 14

Troubleshooting Tips

The following commands can help troubleshoot IP addressing:

- **show ip interface** --Displays the IP parameters for the interface.
- **show ip route connected** --Displays the IP networks the networking device is connected to.

What to Do Next

If your network has two or more routers and you have already configured a routing protocol, make certain that the other routers can reach the new IP network that you assigned. You might need to modify the configuration for the routing protocol on the router so that it advertises the new network. Consult the *Cisco IOS XE IP Routing Configuration Guide* for information on configuring routing protocols:

Using IP Unnumbered Interfaces on Point-to-Point WAN Interfaces to Limit Number of IP Addresses Required

If you have a limited number of IP network or subnet addresses and you have point-to-point WANs in your network, you can use the IP Unnumbered Interfaces feature to enable IP connectivity on the point-to-point WAN interfaces without actually assigning an IP address to them.

Perform this task to configure the IP Unnumbered Interfaces feature on a point-to-point WAN interface.

- IP Unnumbered Feature, page 14
- Troubleshooting Tips, page 12

IP Unnumbered Feature

The IP Unnumbered Interfaces feature enables IP processing on a point-to-point WAN interface without assigning it an explicit IP address. The IP unnumbered point-to-point WAN interface uses the IP address of another interface to enable IP connectivity, which conserves network addresses.

Note The following restrictions apply to the IP Unnumbered Interfaces feature:

- The IP Unnumbered Interfaces feature is only supported on point-to-point (non-multiaccess) WAN interfaces

>

SUMMARY STEPS

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.

	Command or Action	Purpose
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.16.16.1 255.255.240.0`	Configures the IP address on the interface.
Step 6	**interface** *type number* **Example:** `Router(config-if)# interface serial 0/0/0`	Specifies a point-to-point WAN interface and enters interface configuration mode.
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the point-to-point WAN interface.
Step 8	**ip unnumbered** *type number* **Example:** `Router(config-if)# ip unnumbered GigabitEthernet 0/0/0`	Enables the IP unnumbered feature on the point-to-point WAN interface. In this example the point-to-point WAN interface uses IP address 172.16.16.1 from GigabitEthernet 0/0/0.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can help troubleshoot IP addressing:

- **show ip interface** --Displays the IP parameters for the interface.
- **show ip route connected** --Displays the IP networks the networking device is connected to.

Using IP Addresses with 31-Bit Prefixes on Point-to-Point WAN Interfaces to Limit Number of IP Addresses Required

You can reduce the number of IP subnets used by networking devices to establish IP connectivity to point-to-point WANs that they are connected to by using IP Addresses with 31-bit Prefixes as defined in RFC 3021.

Perform this task to configure an IP address with a 31-bit prefix on a point-to-point WAN interface.

- RFC 3021, page 17
- Troubleshooting Tips, page 12

RFC 3021

Prior to RFC 3021, *Using 31-bit Prefixes on IPv4 Point-to-Point Links* , many network administrators assigned IP address with a 30-bit subnet mask (255.255.255.252) to point-to-point interfaces to conserve IP address space. Although this practice does conserve IP address space compared to assigning IP addresses with shorter subnet masks such as 255.255.255.240, IP addresses with a 30-bit subnet mask still require four addresses per link: two host addresses (one for each host interface on the link), one all-zeros network address, and one all-ones broadcast network address.

The table below shows an example of the four IP addresses that are created when a 30-bit (otherwise known as 255.255.255.252 or /30) subnet mask is applied to the IP address 192.168.100.4. The bits that are used to specify the host IP addresses in bold.

Table 8 Four IP Addresses Created When a 30-Bit Subnet Mask (/30) is Used

Address	Description	Binary
192.168.100.4/30	All-zeros IP address	11000000.10101000.01100100.0 0000100 → 11000000.10101000.01100100.000001**00**
192.168.100.5/30	First host addresses	11000000.10101000.01100100.000001**01**
192.168.100.6/30	Second host address	11000000.10101000.01100100.000001**10**
192.168.100.7/30	All-ones broadcast address	11000000.10101000.01100100.000001**11**

Point-to-point links only have two endpoints (hosts) and do not require broadcast support because any packet that is transmitted by one host is always received by the other host. Therefore the all-ones broadcast IP address is not required for a point-to-point interface.

The simplest way to explain RFC 3021 is to say that the use of a 31-bit prefix (created by applying a 31-bit subnet mask to an IP address) allows the all-zeros and all-ones IP addresses to be assigned as host addresses on point-to-point networks. Prior to RFC 3021 the longest prefix in common use on point-to-point links was 30-bits, which meant that the all-zeros and all-ones IP addresses were wasted.

The table below shows an example of the two IP addresses that are created when a 31-bit (otherwise known as 255.255.255.254 or /31) subnet mask is applied to the IP address 192.168.100.4. The bit that is used to specify the host IP addresses in bold

Table 9 Four IP Addresses Created When a 31-Bit Subnet Mask (/31) is Used

Address	Description	Binary
192.168.100.4/31	First host address	11000000.10101000.01100100.000001**0**0

Address	Description	Binary
192.168.100.5/31	Second host address	11000000.10101000.01100100.0 0000101

The complete text for RFC 3021 is available at http://www.ietf.org/rfc/rfc3021.txt .

You must have classless IP addressing configured on your networking device before you configure an IP address with a 31-bit prefix on a point-to-point interface. Classless IP addressing is enabled by default in many versions of Cisco IOS software. If you are not certain that your networking device has IP classless addressing configured, enter the **ip classless** command in global configuration mode to enable it.

Note This task can only be performed on point-to-point (non-multi-access) WAN interfaces.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip classless**
4. **interface** *type number*
5. **no shutdown**
6. **ip address** *ip-address mask*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip classless** **Example:** `Router(config)# ip classless`	(Optional) Enables IP classless (CIDR).

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `Router(config)# interface serial 0/0/0`	Specifies a point-to-point WAN interface and enters interface configuration mode.
Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 192.168.100.4 255.255.255.254`	Configures the 31bit prefix IP address on the point-to-point WAN interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can help troubleshoot IP addressing:

- **show ip interface** --Displays the IP parameters for the interface.
- **show ip route connected** --Displays the IP networks the networking device is connected to.

Maximizing the Number of Available IP Subnets by Allowing the use of IP Subnet Zero

If you using subnetting in your network and you are running out of network addresses, you can configure your networking device to allow the configuration of subnet zero. This adds one more usable network address for every subnet in your IP addressing scheme. The table above shows the IP subnets (including subnet 0) for 172.16.0.0/20.

Perform this task to enable the use of IP subnet zero on your networking device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subnet-zero**
4. **interface** *type number*
5. **no shutdown**
6. **ip address** *ip-address mask*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip subnet-zero** **Example:** `Router(config)# ip subnet-zero`	Enables the use of IP subnet zero.
Step 4	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.

	Command or Action	Purpose
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 172.16.0.1 255.255.240.0`	Configures the subnet zero IP address on the interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

• Troubleshooting Tips, page 12

Troubleshooting Tips

The following commands can help troubleshoot IP addressing:

- **show ip interface** --Displays the IP parameters for the interface.
- **show ip route connected** --Displays the IP networks the networking device is connected to.

Specifying the Format of Network Masks

By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.55 255.255.255.0.

You might find it more convenient to display the network mask in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0XFFFFFF00.

The bit count format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.55/24.

• Specify the Format in Which Netmasks Appear for the Current Session, page 21
• Specify the Format in Which Netmasks Appear for an Individual Line, page 22

Specify the Format in Which Netmasks Appear for the Current Session

Perform this task to specify the format in which netmasks appear for the current session.

SUMMARY STEPS

1. **enable**
2. **term ip netmask-format** {**bitcount** | **decimal** | **hexadecimal**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**term ip netmask-format** {**bitcount** | **decimal** | **hexadecimal**} **Example:** `Router# term ip netmask-format hexadecimal`	Specifies the format the router uses to display network masks.

Specify the Format in Which Netmasks Appear for an Individual Line

Perform this task to specify the format in which netmasks appear for an individual line.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty** *first last*
4. **term ip netmask-format** {**bitcount** | **decimal** | **hexadecimal**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**line vty** *first last* **Example:** `Router(config)# line vty 0 4`	Enters line configuration mode for the range of lines specified by the *first* and *last* arguments.
Step 4	**term ip netmask-format** {**bitcount** | **decimal** | **hexadecimal**} **Example:** `Router(config-line)# ip netmask-format hexadecimal`	Specifies the format the router uses to display the network mask for an individual line.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuration Examples for IP Addresses

Establishing IP Connectivity to a Network by Assigning an IP Address to an Interface Example

The following example configures an IP address on three interfaces:

```
!
interface GigabitEthernet0/0/0
 no shutdown
 ip address 172.16.16.1 255.255.240.0
!
interface GigabitEthernet0/0/1
 no shutdown
 ip address 172.16.32.1 255.255.240.0
!
```

```
interface GigabitEthernet0/0/2
 no shutdown
 ip address 172.16.48.1 255.255.240.0
!
```

Increasing the Number of IP Hosts that are Supported on a Network by Using Secondary IP Addresses Example

The following example configures secondary IP addresses on three interfaces:

```
!
interface GigabitEthernet0/0/0
 no shutdown
 ip address 172.16.16.1 255.255.240.0
 ip address 172.16.32.1 255.255.240.0 secondary
!
!
interface GigabitEthernet0/0/1
 no shutdown
 ip address 172.17.16.1 255.255.240.0
 ip address 172.17.32.1 255.255.240.0 secondary
!
!
interface GigabitEthernet0/0/2
 no shutdown
 ip address 172.18.16.1 255.255.240.0
 ip address 172.18.32.1 255.255.240.0 secondary
!
```

Example Using IP Unnumbered Interfaces on Point-to-Point WAN Interfaces to Limit Number of IP Addresses Required

The following example configures the unnumbered IP feature on three interfaces:

```
!
interface GigabitEthernet0/0/0
 no shutdown
 ip address 172.16.16.1 255.255.240.0
!
interface serial0/0/0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
!
interface serial0/0/1
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
!
interface serial0/0/2
 no shutdown
 ip unnumbered fastethernet0/0
!
```

Example Using IP Addresses with 31-Bit Prefixes on Point-to-Point WAN Interfaces to Limit Number of IP Addresses Required

The following example configures 31-bit prefixes on two interfaces:

```
!
ip classless
!
interface serial0/0/0
```

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

Maximizing the Number of Available IP Subnets by Allowing the use of IP Subnet Zero Example

The following example enables subnet zero:

```
!
interface GigabitEthernet0/0/0
 no shutdown
 ip address 172.16.16.1 255.255.240.0
!
ip subnet-zero
!
```

Where to Go Next

If your network has two or more routers and you have not already configured a routing protocol, consult the appropriate *Cisco IOS XE IP Routing Configuration Guide*, for details on configuring routing protocols.

Additional References

The following sections provide references related to IP Addresses.

Related Documents

Related Topic	Document Title
IP addressing commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
Fundamental principles of IP addressing and IP routing	IP Routing Primer ISBN 1578701082

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified	--

RFCs

RFC[6]	Title
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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

6 These references are only a sample of the many RFCs available on subjects related to IP addressing and IP routing. Refer to the IETF RFC site at http://www.ietf.org/rfc.html for a full list of RFCs.

Feature Information for IP Addresses

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10 Feature Information for IP Addresses

Feature Name	Releases	Feature Information
Using 31-bit Prefixes on IP Point-to-Point Links	Cisco IOS XE Release 2.1	In order to conserve IP address space on the Internet, a 31-bit prefix length allows the use of only two IP addresses on a point-to-point link. Previously, customers had to use four IP addresses or unnumbered interfaces for point-to-point links.
IP Unnumbered Interfaces	Cisco IOS XE Release 2.1	In order to conserve IP address space, IP unnumbered interfaces use the IP address of another interface to enable IP connectivity. The following command was introduced or modified: **ip unnumbered**.
IP Subnet Zero	Cisco IOS XE Release 2.1	In order to conserve IP address space IP Subnet Zero allows the use of the all-zeros subnet as an IP address on an interface, such as configuring 172.16.0.1/24 on GigabitEthernet 0/0/0. The following command was introduced or modified: **ip subnet-zero**.

Feature Name	Releases	Feature Information
Classless Inter-Domain Routing	Cisco IOS XE Release 2.1	CIDR is a new way of looking at IP addresses that eliminates the concept of classes (class A, class B, and so on). For example, network 192.213.0.0, which is an illegal class C network number, is a legal supernet when it is represented in CIDR notation as 192.213.0.0/16. The /16 indicates that the subnet mask consists of 16 bits (counting from the left). Therefore, 192.213.0.0/16 is similar to 192.213.0.0 255.255.0.0. The following command was introduced or modified: **ip classless**.

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: 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)

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

IP Overlapping Address Pools

The IP Overlapping Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP Overlapping Address Pools

The Cisco IOS XE software checks for duplicate addresses on a per-group basis. The check for duplicate addresses means that you can configure pools in multiple groups that could have possible duplicate addresses. The IP Overlapping Address Pools feature should be used only in cases where overlapping IP address pools make sense, such as Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environments where multiple IP address spaces are supported.

Information About IP Overlapping Address Pools

Benefits

The IP Overlapping Address Pools gives greater flexibility in assigning IP addresses dynamically. It allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

How IP Address Groups Work

IP Control Protocol (IPCP) IP pool processing implements all IP addresses as belonging to a single IP address space, and a given IP address should not be assigned multiple times. IP developments such as virtual private dialup network (VPDN) and Network Address Translation (NAT) implement the concept of multiple IP address spaces where it can be meaningful to reuse IP addresses, although such usage must ensure that these duplicate address are not placed in the same IP address space. An IP address group to support multiple IP address spaces and still allow the verification of nonoverlapping IP address pools within a pool group. Pool names must be unique within the router. The pool name carries an implicit group identifier because that pool name can be associated only with one group. Pools without an explicit group name are considered members of the base system group and are processed in the same manner as the original IP pool implementation.

Existing configurations are not affected by the new pool feature. The “group” concept is an extension of the existing **ip local pool** command. Processing of pools that are not specified as a member of a group is unchanged from the existing implementation.

How to Configure IP Overlapping Address Pools

Configuring and Verifying a Local Pool Group

Perform this task to configure a local pool group and verify that it exists.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip local pool** {**default** | *poolname*} {*low-ip-address* [*high-ip-address*] [**group** *group-name*] [**cache-size** *size*]}
4. **show ip local pool** [*poolname* | [**group** *group-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip local pool** {**default** | *poolname*} {*low-ip-address* [*high-ip-address*] [**group** *group-name*] [**cache-size** *size*]} **Example:** `Router(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000`	Configures a group of local IP address pools, gives this group a name, and specifies a cache size.
Step 4	**show ip local pool** [*poolname* | [**group** *group-name*]] **Example:** `Router(config)# show ip local pool group testgroup testpool`	Displays statistics for any defined IP address pools.

Configuration Examples for Configuring IP Overlapping Address Pools

Define Local Address Pooling as the Global Default Mechanism Example

The following example shows how to configure local pooling as the global default mechanism:

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

Configure Multiple Ranges of IP Addresses into One Pool Example

The following example shows how to configure two ranges of IP addresses for one IP address pool:

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

Additional References

The following sections provide references related to configuring IP Overlapping Address Pools.

Related Documents

Related Topic	Document Title
Dial commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Dial Services Command Reference*
IP address pooling	"Configuring Media-Independent PPP and Multilink PPP" chapter of the Cisco IOS XE Dial Technologies Configuration Guide

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 826	*Address Resolution Protocol*
RFC 903	*Reverse Address Resolution Protocol*

RFCs	Title
RFC 1027	*Proxy Address Resolution Protocol*
RFC 1042	*Standard for the Transmission of IP Datagrams over IEEE 802 Networks*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring IP Overlapping Address Pools

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11 Feature Information for Configuring IP Overlapping Address Pools

Feature Name	Releases	Feature Information
IP Overlapping Address Pools	Cisco IOS XE Release 2.1	The IP Overlapping Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces. The following commands were modified by this feature:**ip local pool**and **show ip local pool.**

Glossary

IPCP --IP Control Protocol. Protocol that establishes and configures IP over PPP.

MPLS --Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

NAT --Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

VPDN --virtual private dialup network. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost-effective method of establishing a long distance, point-to-point connection between remote dial users and a private network. See also VPN.

VPN --Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VRF --A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

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: 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)

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