Fundamentals of IPv4 Addressing and Routing

Prof. Ashwini Mathur

OSI

The OSI physical layer **(Layer 1)** defines how to transmit bits over a particular type of physical network.

The OSI data link layer **(Layer 2)** defines the **framing, addressing, error detection**, and **rules for when to use the physical medium**.

Although they are important, **these two layers do not define how to deliver data between devices that exist far from each other**, with many different physical networks sitting between the two computers.

OSI Layer 3-equivalent protocols

This define how packets can be delivered from the computer that creates the packet all the way to the computer that needs to receive the packet. To reach that goal, an OSI network layer protocol defines the following features:

Routing: The process of forwarding packets (Layer 3 PDUs).

Logical addressing: Addresses that can be used regardless of the type of physical networks used, providing each device (at least) one address. Logical addressing enables the routing process to identify a packet's source and destination.

Routing protocol: A protocol that aids routers by dynamically learning about the groups of addresses in the network, which in turn allows the routing (forwarding) process to work well.

Other utilities: The network layer also relies on other utilities. For TCP/IP, these utilities include Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and ping.

NOTE : The term path selection sometimes is used to mean the same thing as routing protocol, sometimes is used to refer to the routing (forwarding) of packets, and sometimes is used for both functions.


IP Phone
Phone
Cisco CallManager
100BaseT Hub
Wireless Router
Route/Switch Processor
Cisco ASA 5500
Printer
Cisco 5500 Family
Access Point
Router
Workgroup Switch
PC
Laptop
Modem
Headquarters
Branch Office
File/ Application Server
Hub
Network Cloud
Line: Ethernet

IP Addressing Definitions

If a device wants to communicate using TCP/IP, it needs an IP address. When the device has an IP address and the appropriate software and hardware, it can send and receive IP packets. Any device that can send and receive IP packets is called an *IP host*.

Understand IP Address

An IP address is an address used in order to **uniquely identify a device** on an IP network.

The address is made up of **32 binary bits**, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets **(1 octet = 8 bits)**. Each octet is converted to decimal and separated by a period (dot).

For this reason, an IP address is said to be expressed in **dotted decimal format** (for example, 172.16.81.100). The value in each **octet ranges from 0 to 255** decimal, or 00000000 - 11111111 binary

In a **Class A address**, the **first octet is the network portion**, so the Class A example in Figure 1 has a major network address of 1.0.0.0 - 127.255.255.255.

Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a **Class B address**, the f**irst two octets are the network portion**, so the Class B example in Figure 1 has a major network address of 128.0.0.0 - 191.255.255.255. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses are used for networks that have between 256 and 65534 hosts.

In a **Class C address,** the **first three octets are the network portion**. The Class C example in Figure 1 has a major network address of 192.0.0.0 - 223.255.255.255. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

Table 5-3 *Sizes of Network and Host Parts of IP Addresses with No Subnetting*

Any Network of This Class	Number of Network Bytes (Bits)	Number of Host Bytes (Bits)	Number of Addresses Per Network*
A	1 (8)	3 (24)	$2^{24} - 2$
B	2 (16)	2 (16)	$2^{16} - 2$
C	3 (24)	1 (8)	$2^{8} - 2$

*There are two reserved host addresses per network.

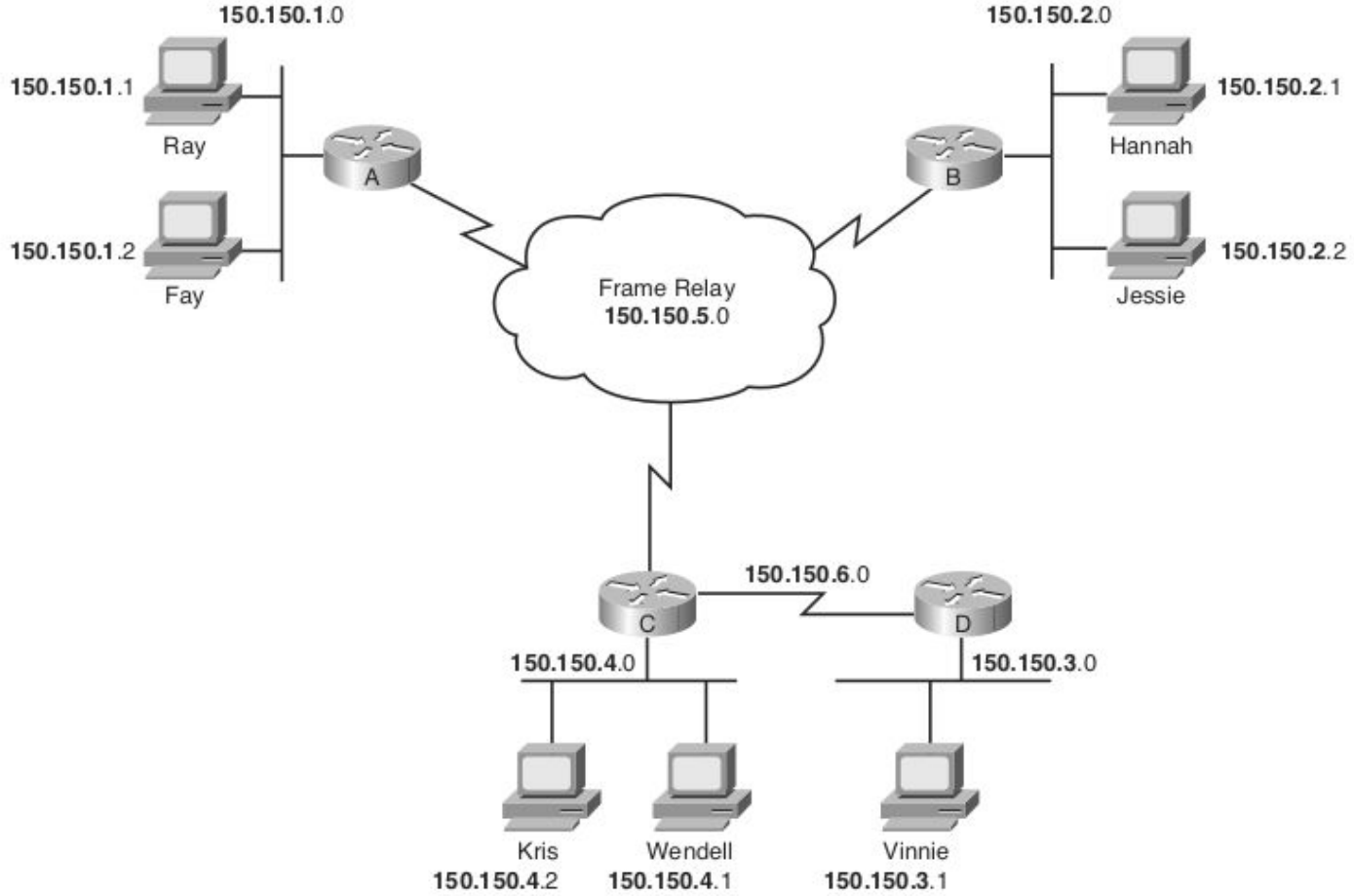
Table 5-5 *All Possible Valid Network Numbers*[*]

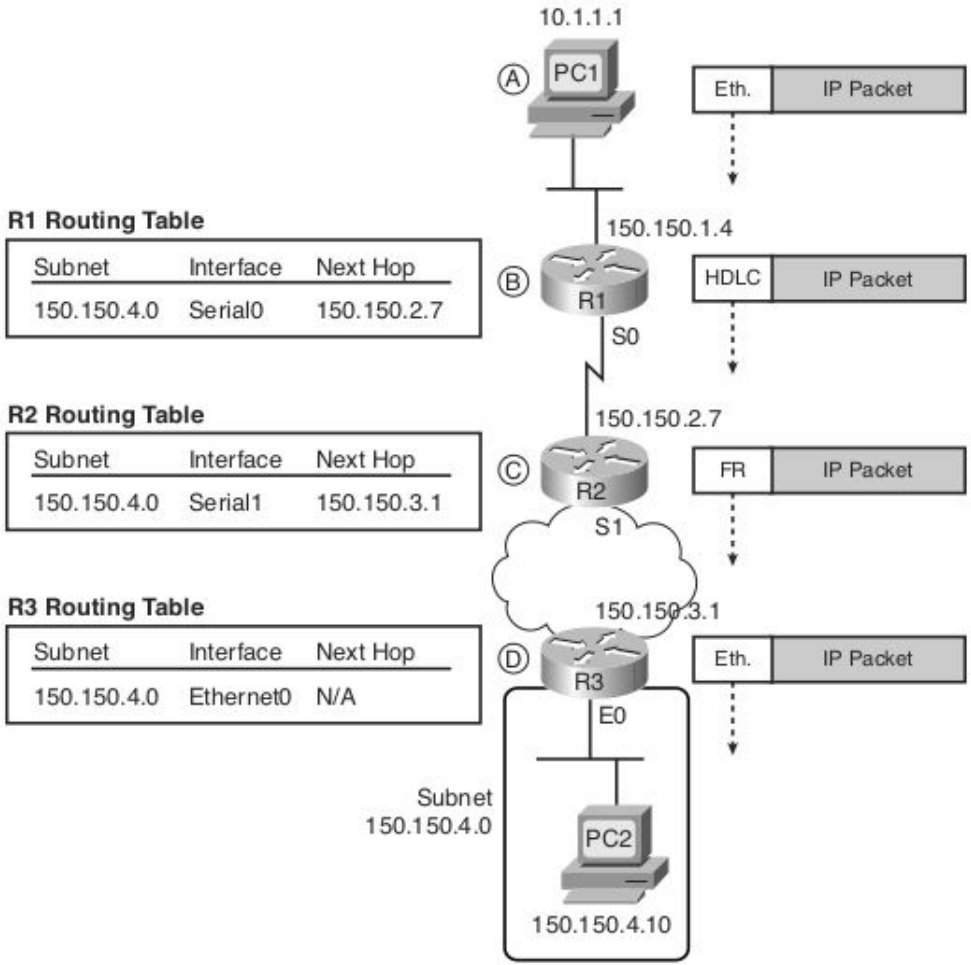
Class	First Octet Range	Valid Network Numbers[*]	Total Number for This Class of Network	Number of Hosts Per Network
A	1 to 126	1.0.0.0 to 126.0.0.0	$2^7 - 2$ (126)	$2^{24} - 2$ (16,777,214)
B	128 to 191	128.0.0.0 to 191.255.0.0	2^{14} (16,384)	$2^{16} - 2$ (65,534)
C	192 to 223	192.0.0.0 to 223.255.255.0	2^{21} (2,097,152)	$2^8 - 2$ (254)

Table 5-4 *Sample Network Numbers, Decimal and Binary*

Network Number	Binary Representation, with the Host Part in Bold
8.0.0.0	00001000 **00000000 00000000 00000000**
130.4.0.0	10000010 00000100 **00000000 00000000**
199.1.1.0	11000111 00000001 00000001 **00000000**

Figure 5-6 *Using Subnets*

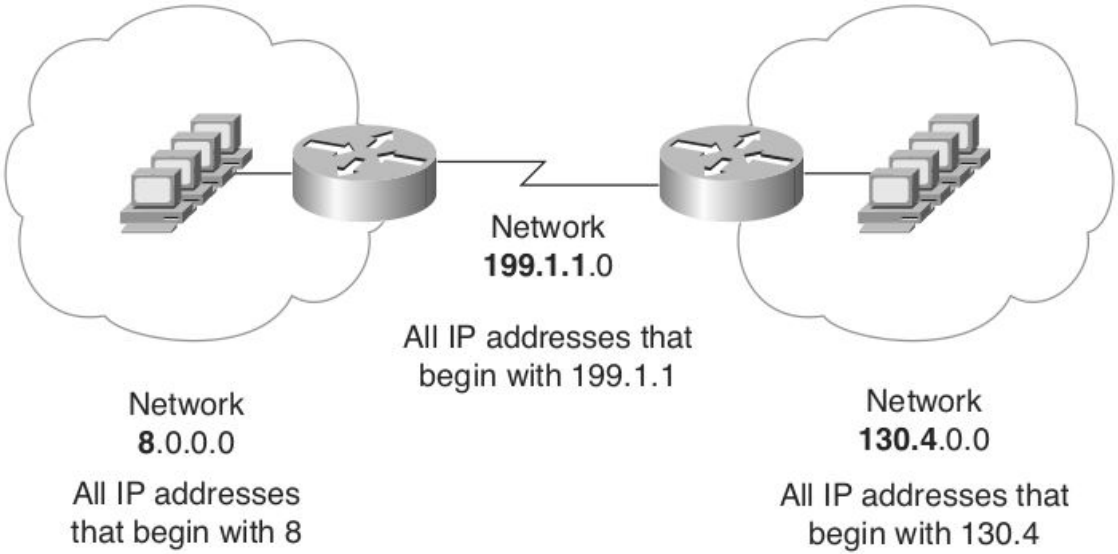


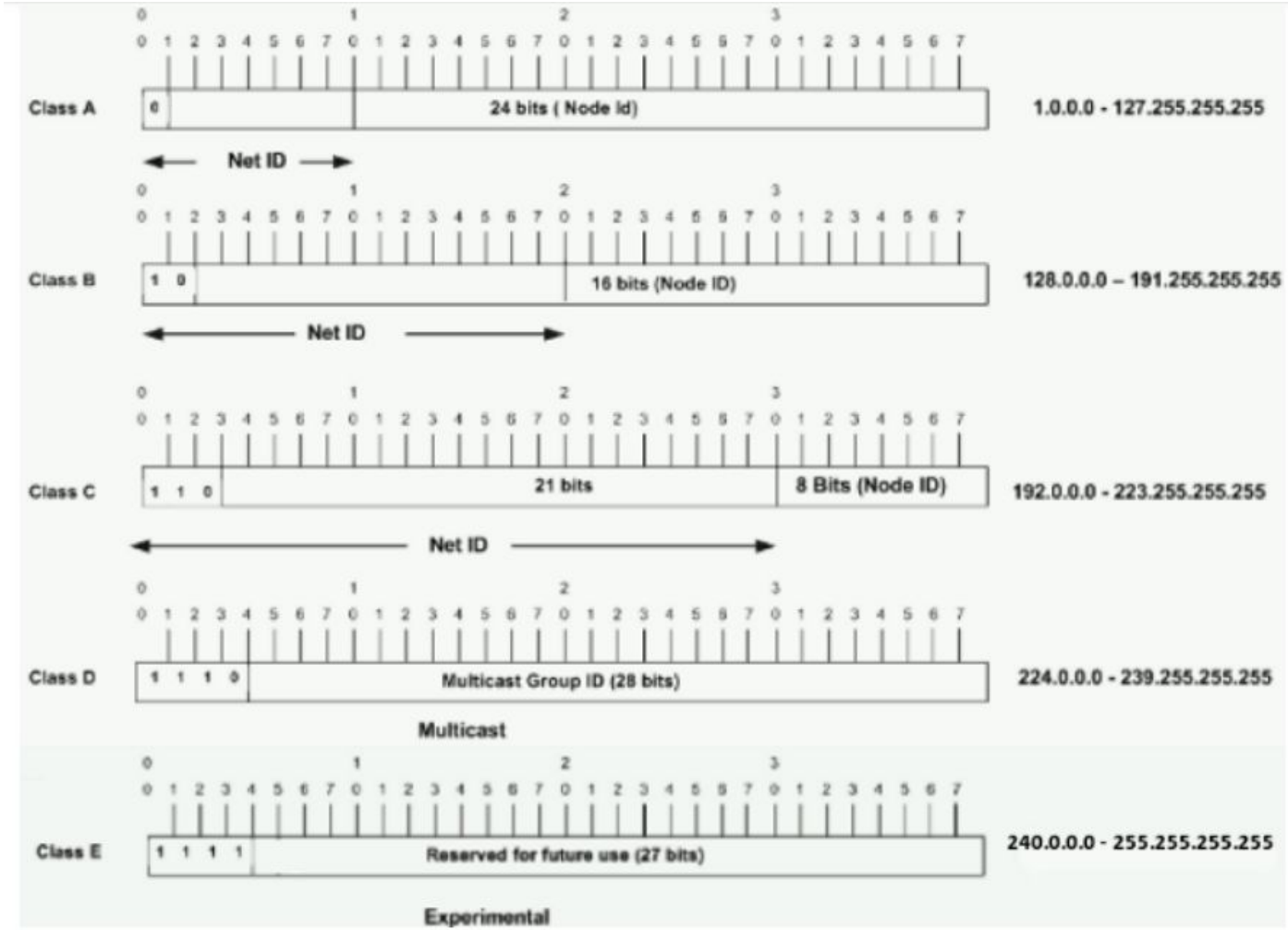

10.1.1.1
A
PC1
Eth.
IP Packet
150.150.1.4
B
R1
HDLC
IP Packet
S0
150.150.2.7
C
R2
FR
IP Packet
S1
150.150.3.1
D
R3
Eth.
IP Packet
E0
Subnet
150.150.4.0
PC2
150.150.4.10
R1 Routing Table
Subnet Interface Next Hop
150.150.4.0 Serial0 150.150.2.7
R2 Routing Table
Subnet Interface Next Hop
150.150.4.0 Serial1 150.150.3.1
R3 Routing Table
Subnet Interface Next Hop
150.150.4.0 Ethernet0 N/A

How IP Addresses Are Grouped

The original specifications for TCP/IP grouped IP addresses into sets of consecutive addresses called *IP networks*. The addresses in a single network have the same numeric value in the first part of all addresses in the network. Figure 5-4 shows a simple internetwork that has three separate IP networks.

Figure 5-4 *Sample Network Using Class A, B, and C Network Numbers*




Class A
0
24 bits (Node Id)
1.0.0.0 - 127.255.255.255
Net ID
Class B
1 0
16 bits (Node ID)
128.0.0.0 – 191.255.255.255
Net ID
Class C
1 1 0
21 bits
8 Bits (Node ID)
192.0.0.0 - 223.255.255.255
Net ID
Class D
1 1 1 0
Multicast Group ID (28 bits)
224.0.0.0 - 239.255.255.255
Multicast
Class E
1 1 1 1
Reserved for future use (27 bits)
240.0.0.0 - 255.255.255.255
Experimental

Network Masks

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node.

Class A, B, and C networks have default masks, also known as natural masks, as shown here:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Example

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0.

In order to see how the mask helps you **identify the network and Host parts** of the address,

Convert the address and mask to binary numbers.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = **11111111**.00000000.00000000.00000000

Once you have the address and the mask represented in binary, then identification of the network and host ID is easier. Any address bits which have corresponding **mask bits set to 1 represent the network ID**.

Any address bits that have corresponding **mask bits set to 0 represent the node ID**.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000 ----------

net id | **host id**

netid = 00001000 = **8** , **hostid** = 00010100.00001111.00000001 = **20.15.1**

Understand Subnetting ..

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network.

If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks.

Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects n networks/subnetworks has n distinct IP addresses, one for each network / subnetwork that it interconnects.

Subnet Network

In order to subnet a network, **extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID**.

For example,

Given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

204.17.5.0 - 11001100.00010001.00000101.00000000

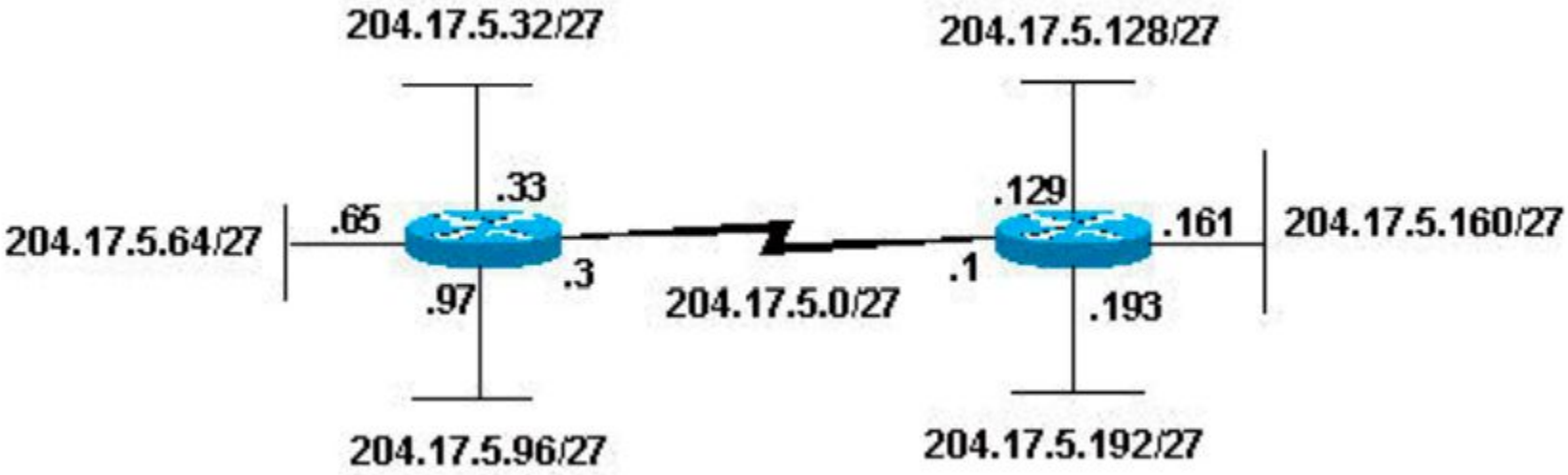
255.255.255.224 - 11111111.11111111.11111111.**111**00000 **|sub|**

Subnetting ..

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets.

With **these three bits, it is possible to create eight subnets**. With the remaining five host ID bits, **each subnet can have up to 32 host addresses**, 30 of which can actually be assigned to a device since **host ids of all zeros or all ones are not allowed** (it is very important to remember this). So, with this in mind, these subnets have been created.

204.17.5.0	255.255.255.224	host address range 1 to 30
204.17.5.32	255.255.255.224	host address range 33 to 62
204.17.5.64	255.255.255.224	host address range 65 to 94
204.17.5.96	255.255.255.224	host address range 97 to 126
204.17.5.128	255.255.255.224	host address range 129 to 158
204.17.5.160	255.255.255.224	host address range 161 to 190
204.17.5.192	255.255.255.224	host address range 193 to 222
204.17.5.224	255.255.255.224	host address range 225 to 254


204.17.5.32/27
204.17.5.128/27
204.17.5.64/27
.65
.33
.129
.161
204.17.5.160/27
.3
.1
204.17.5.0/27
.97
.193
204.17.5.96/27
204.17.5.192/27

Note

Note: There are two ways to denote these masks. First, since you use three bits more than the "natural" Class C mask, you can denote these addresses as having a 3-bit subnet mask. Or, secondly, the mask of 255.255.255.224 can also be denoted as /27 as there are 27 bits that are set in the mask. This second method is used with CIDR. With this method, one of these networks can be described with the notation prefix/length. For example, 204.17.5.32/27 denotes the network 204.17.5.32 255.255.255.224. When appropriate, the prefix/length notation is used to denote the mask throughout the rest of this document.

Note

Note: In the past, there were limitations to the use of a subnet 0 (all subnet bits are set to zero) and all ones subnet (all subnet bits set to one). Some devices would not allow the use of these subnets. Cisco Systems devices allow the use of these subnets when the ip subnet zero command is configured.