COURSE SAMPLE: IPV4 ADDRESSES

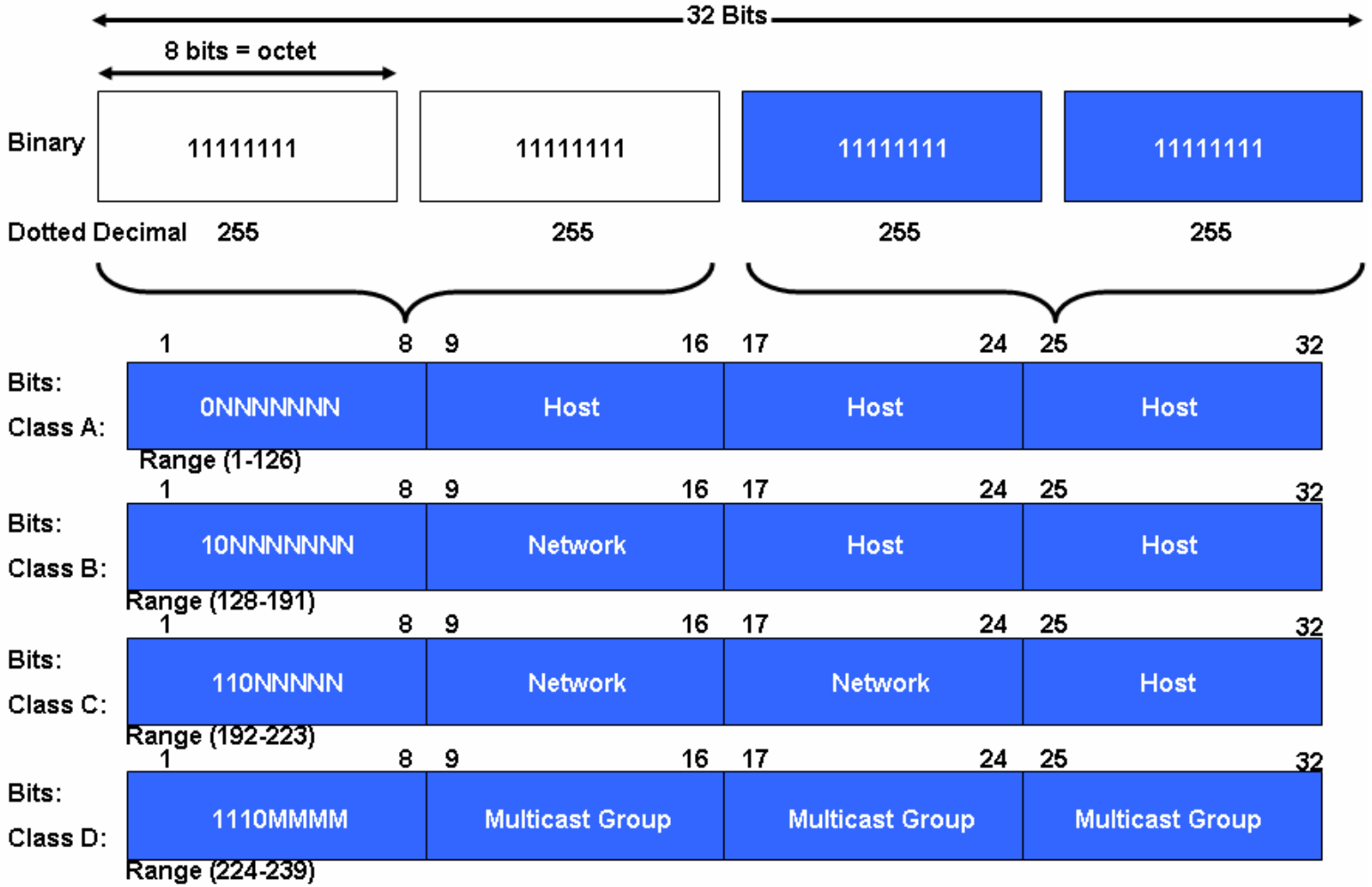
This document is protected by copyright law.

It is provided free of charge as a download from the Technology Training Limited website for personal use only.

It may not be reproduced in any format without written permission from a Director of Technology Training Ltd.

© Technology Training Limited

IP Address Classes



© Technology Training Limited

1.1.1 Conventional IP Addresses

IP addresses in IPv4 are 32 bits long, and are often written in dotted decimal notation, where each byte is represented by a decimal number between 0 and 255, and these values are separated by a period (a full stop), for example 192.168.11.4.

The address for a specific host must have a unique 32-bit address and this is composed from a network prefix and a host part. All of the hosts within a network share a common network prefix, and each host within a network must have a unique host part of the overall address[1]. The boundary between the network part and the host part of the address can occur at different places within the overall 32-bit address, and where this boundary lies for a specific host is defined by the mask for the address. Traditionally these addresses have been defined by network prefixes ending on each of the byte boundaries within the addressing field:

- Class A addresses use the most significant byte for the network part and the three remaining bytes for the host part of the address
- Class B addresses use the most significant two bytes for the network part, and the remaining bytes for the host part of the address
- Class C addresses use the most significant three bytes for the network part, and the remaining byte for the host part of the address
- Class D addresses are special addresses reserved for multicast; many hosts can listen on the same multicast address for packets sent from one sender.

[1] All hosts with the same network part of their address must be directly connected, in other words cannot have a router between them. All hosts with a different network part of their address cannot be directly connected, and must have a router between them. Following this logic, then the different interfaces on a router must each belong to a different network, and have a different network part of their address, since the router lies between them!

© Technology Training Limited

All Possible Valid Network Numbers*

Class	First Octet Range	Valid Network Numbers*	Total Networks for This Class	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)

* The Valid Network Numbers column shows actual network numbers. Networks 0.0.0.0 (originally defined for use as a broadcast address) and 127.0.0.0 (still available for use as the loopback address) are reserved.

© Technology Training Limited

1.1.2 Classful Address Ranges

The Table opposite shows the available network addresses for each classful network.[2]

[2] Network 0.0.0.0 is reserved for broadcasts, and 127.0.0.0 is reserved for loopback use, therefore the allowed class A range is 1.0.0.0 to 126.0.0.0.

© Technology Training Limited

RFC 1918 Private Address Space

Private IP Networks	Class of Networks	Number of Networks
10.0.0.0 through 10.0.0.0	A	1
172.16.0.0 through 172.31.0.0	B	16
192.168.0.0 through 192.168.255.0	C	256

© Technology Training Limited

1.1.3 Reserved IP Addresses

Certain addresses are reserved for special use in IP networks:

- The class A network 127.0.0.0 255.0.0.0 is reserved for loopback use. Packets sent to this address are never presented on the physical interface; instead they are looped back by the TCP/IP stack and presented to the appropriate application on the originating host. So, for example, a host running an ftp server and an ftp client could connect to the local FTP server by using 127.0.0.1 as the destination host address. This approach is sometimes used to test applications without involving a physical network or remote host.
- A Directed Broadcast address has all of the host bits in a particular network set to (binary) 1, and is used to send a packet to all hosts on the network. So for example the destination address 192.168.1.255 is a directed broadcast to all of the hosts in network 192.168.1.0 255.255.255.0
- A Local Broadcast address is used to send a packet to all hosts on the local network, and has all address bits set to (binary) 1. So the destination address 255.255.255.255 sent by a host on network 192.168.1.0 255.255.255.0 would send a packet to all hosts on the local network

1.1.4 Private IP Addresses

RFC 1918 defines a collection of IP addresses which are reserved for private use. These addresses are not routable across the public Internet, but can be freely used within private networks[3]. If private networks using these ranges need to communicate across the public Internet, they must use some technique for hiding or converting their private addresses, such as Network Address Translation (NAT) or tunnelling.

The RFC1918 private address ranges are listed below:

- 10.0.0.0 to 10.255.255.255 (a single class A network)
- 172.16.0.0 to 172.31.255.255 (16 class B networks)
- 192.168.0.0 to 192.168.255.255 (256 class B networks)

[3]Home users who have an ADSL or cable modem router to connect to the Internet, and can connect multiple PCs on the LAN side of their device typically use RFC1918 addresses provided by their router.

© Technology Training Limited