
Section 1 -- Introduction

Thank you for purchasing the Network Safety Corporation (NSC) NetNAT Internet Firewall. The NetNAT uses Network Address Translation and our own innovative technology to reduce your need for public IP addresses, protect your network from outsiders, and eliminate periodic network renumbering due to a change in ISP. The NetNAT vastly reduces the number of registered IP addresses a private network needs to gain access to or receive service requests from the Internet.

NetNAT Features

The NetNAT is an IP Firewall and Network Address Translation (NAT) facility. It also acts as the gateway between your private Intranet and the public Internet. The NetNAT supports the following features:

- ◆ Firewall Protection
- ◆ Ten different modes of Network Address Translation
- ◆ IP Routing and Internet Gateway
- ◆ Multiple Service Mapping Modes
- ◆ Virtual Private Networks
- ◆ User Internet Access Control
- ◆ Four Built-in Servers
- ◆ Hardware Watchdog Timer
- ◆ Syslog -- Event and Volume Logging
- ◆ Network Monitoring

Planning Your Installation

The next few sections discuss basic information that you will need in the planning of your NetNAT installation. The Internet Protocol will be discussed briefly, as will be IP addressing, sub-netting and routing. We will describe a few of the protocols that use IP for their transport, as well as a few of the current Internet applications.

IP Addresses

An IP Address consists of a 32-bit number that was intended to be unique throughout the world. Every computer that uses IP must have an IP Address. This 32-bit number is usually expressed or written as four decimal numbers separated by dots. Each number may range from 0 through 255, since each represents an 8-bit value, so that all four together represent the whole 32-bit number. All of this helps to minimize the wear and tear on our minds caused by mental conversion between hex and decimal. Here are some examples:

Dotted Decimal	Hexadecimal	Binary
172.17.33.116	0xAC112174	10101100000100010010000101110100
192.168.2.7	0xC0A80207	11000000101010000000001000000111
10.99.61.25	0x0A633D19	00001010011000110011110100011001
207.68.156.49	0xCF449C31	11001111010001001001110000110001

You can see why they devised the “Dotted Decimal” notation form! Fortunately, we are not required to memorize IP Addresses very often. In general, we just need to remember our own “network address.”

Network Addresses

In the context of IP Routing, a Network is a virtual place where the “network part” of the IP Addresses of every workstation and host are exactly the same, differing only in the “host part.” For example, if an organization has a single LAN with a single Class C Network, say, 192.168.2.0, then every IP Address in that network will start with the same 24 bits or three octets: 192.168.2. The remaining octet provides space for 256 unique addresses, some of which are reserved. The 192.168.2 is the “network part” of the address; the final octet is the “host part.”

In addition, we need the concept of a “netmask.” This array of bits contains “one bits” in each position of the network part. As its name implies, the netmask is the tool that computers use to extract the network part from a complete IP Address. They “AND” the IP Address with the netmask to get just the network part. AND is a computer process that keeps bits where the mask is made of ones, and drops bits where the mask is zero. In this example, where the network part is 24-bits long, the netmask consists of 24 “one bits” and 8 “zero bits,” so we keep the first 24 bits and clear the last 8.

Here are examples of IP Addresses, netmasks and the network part resulting from an AND operation:

IP Address	Netmask	Network Part
192.168.31.96	255.255.255.0	192.168.31.0
207.68.156.49	255.255.255.0	207.68.156.0
86.115.50.211	255.255.0.0	86.115.0.0

These examples show netmasks whose sections are all multiples of 8-bits. While these are easiest for your user to remember and understand, only the simplest of networks use these exclusively. That is not to say that a simple network is bad. Let us give praise to the network designer that can create a simple, understandable network, for that network will be far easier to understand and maintain.

Netmask Representation

The industry is moving in the direction of simplified representation of netmasks. The traditional representations are either dotted decimal or hexadecimal, with different systems having different standards or even several standards. These traditional forms have persisted due to pure inertia, and usage by some network designers of so-called “comb” netmasks, where “zero bits” are interspersed with the one bits, creating very complex, overlapping sub-networks. This practice is greatly discouraged, since it creates networks that are very difficult to understand and debug.

Assuming that we won't be creating comb netmasks, a shorthand representation of the netmask can be simply the number of one bits in the mask. For example, the natural netmask for a Class-C network (255.255.255.0) could be represented by 24, since there are twenty-four one bits in the mask. So, a Class-C network with the network part of 204.86.17.0 that is not subnetted would be expressed as 204.86.17/24 or 204.86.17.0/24. This notation is gathering widespread support, and will be used frequently in the NetNAT configuration commands.

Something you may see that conflicts with this representation is the expression chosen for indicating multiple Class-C networks combined into a super-net. This is part of the CIDR initiative (Classless Internet Domain Routine), and looks like 204.86.17.0/3, which means three consecutive Class-C networks beginning with 204.86.17.0. You can tell which notation is intended by applying the common sense approach, since if the 3 in this example were a netmask length, the resulting network part would be 192.0.0.0.

Tables of Netmasks

Here are tables of netmasks, mask widths in bits, host part widths in bits and effective number of computer addresses in each size network (after excluding the two reserved broadcast addresses of all-zeros and all-ones).

Netmasks for Large Sub-Networks

Netmask	# Bits in Net Part	# Bits in Host Part	Max Hosts	Netmask	# Bits in Net Part	# Bits in Host Part	Max Hosts
255.255.0.0	16	16	65,534	255.255.240.0	20	12	4094
255.255.128.0	17	15	32,766	255.255.248.0	21	11	2046
255.255.192.0	18	14	16,382	255.255.252.0	22	10	1022
255.255.224.0	19	13	8,046	255.255.254.0	23	9	510

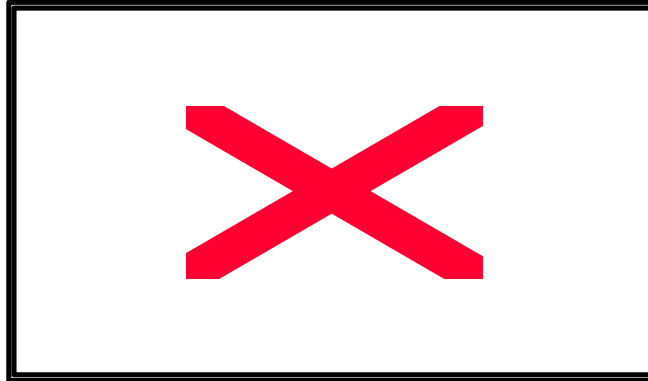
Netmasks for Smaller Sub-Networks

Netmask	# Bits in Net Part	# Bits in Host Part	Max Hosts	Netmask	# Bits in Net Part	# Bits in Host Part	Max Hosts
255.255.255.0	24	8	254	255.255.255.240	28	4	14
255.255.255.128	25	7	126	255.255.255.248	29	3	6
255.255.255.192	26	6	62	255.255.255.252	30	2	2
255.255.255.224	27	5	30	255.255.255.254	31	1	0

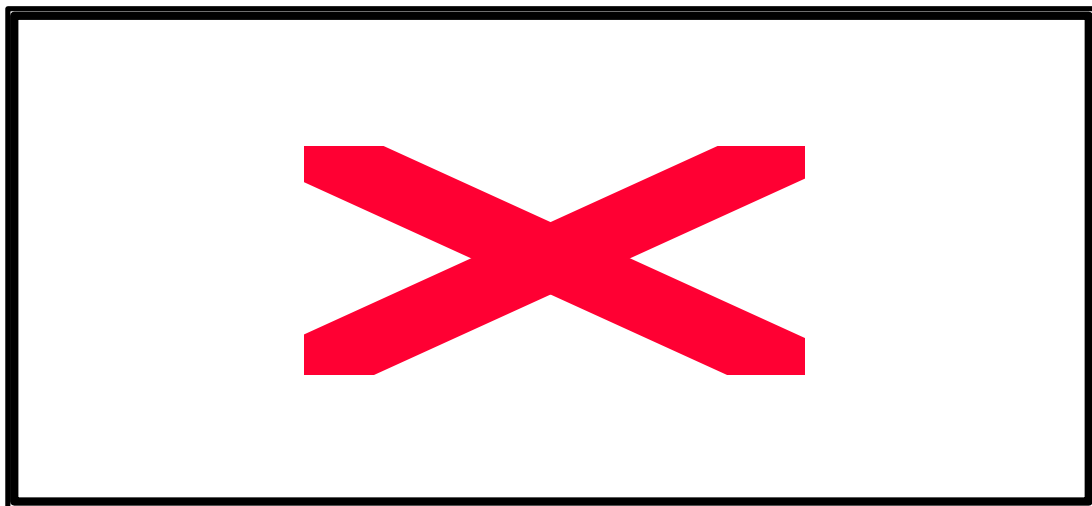
Most designers strive to use a 24-bit netmasks for user subnets, with 23-bit netmasks used in rare cases, where more hosts must be accommodated. Smaller subnets (wider netmasks) are used for smaller offices and for Wide Area Network links. A 30-bit netmask works well on point-to-point WAN links, since it provides for a single IP Address for each end of the link. A 26-bit netmask provides for up to 62 computers on a small office LAN.

IP Routing

The rules of IP routing are very simple. If two computers are in a single network (the “network parts” of their IP Addresses are the same), they may communicate directly with each other:



If the two computers are in different networks, they need at least one router to communicate. A router’s job is to interconnect networks. A router will be a member of a network (having an IP Address within that network), and knows routes to other networks. In the next drawing, there are two networks interconnected by a single router. The router interface in Network A has an IP Address from Network A; the interface in Network B has an IP Address from Network B. The devices in Network A are told that the router’s interface in their network is their “default gateway,” or their route to the outside world. The same is done for the devices in Network B, except that the router’s interface in their network is specified.



Packing List

Use the list below when unpacking the NetNAT components to ensure you have received all the correct items:

- ◆ 1 3.5" diskette labeled NetNAT Software
- ◆ 2 Fast-Ethernet controllers with utility diskette
- ◆ License Document
- ◆ Product Registration card
- ◆ This manual

Contacting Customer Support

Email is the best way to contact NSC. We use the Internet for everything we can!

E-Mail

Customer Support	nscsupport@safety.net
General Information	sales@safety.net
Sales	sales@safety.net
Webmaster	webmaster@safety.net

Phone

602-585-4040

FAX

602-585-7257

Mailing Address

Network Safety Corp.
5831 E. Dynamite Blvd.
Cave Creek, AZ 85331-3435