How to Shut Off IP Forwarding

The Network Information Center
of the University of Texas at Austin (UT NIC)

Document version 1.0

Introduction

This document describes how to shut off IP forwarding in SunOS systems and other UNIX systems. IP forwarding is a routing mechanism in the TCP/IP protocol suite that is used by gateway systems to forward IP datagrams onto their correct destination. If IP forwarding is enabled for standard hosts with single network interfaces, it allows those hosts to produce unnecessary packets in response to broadcast messages on the network. These excess packets can build up to large levels and cause what is known as a network ‘‘broadcast storm.’’

The smooth operation of the UTnet system requires that all hosts not used as gateways disable IP forwarding. This is the default setting in all currently shipped UNIX systems based on the BSD 4.3 release of UNIX.

1. Why Shut Off IP Forwarding?

IP forwarding refers to the ability of most TCP/IP implementations to receive datagrams on one network interface and send them out on another interface, assuming the machine has multiple network interfaces. This means that a given TCP/IP host can function as a rudimentary gateway if it has more than one interface.

As a side effect of this ability, a host can also forward packets back out the interface on which they were originally received. This is a gateway function that is performed by true dedicated gateway machines when they want to forward a datagram to another gateway for routing. In the past, single-homed UNIX hosts (i.e. machines with just one interface) were frequently left with software that gave them the ability to forward packets back out the single interface as part of the original TCP/IP implementations on UNIX.

This ability proved to be a bad idea, since it allowed hosts to add to the broadcast storm problem by sending a broadcast packet that they could not route back out onto the network they received it from, usually in concert with a hundred or so other systems doing the same thing. The end result was one component of the transient network overloads known as broadcast storms.

Most modern host implementations have been fixed, and are no longer capable of forwarding packets or otherwise performing gateway functions when they have only one interface. However, older host implementations can still cause problems in this way.

2. How to Shut Off IP Forwarding in SunOS.

The directions in this document show how to use the *adb* utility under SunOS to set the value of the *ipforwarding* variable in the SunOS kernel to zero, and thereby shut off the ability of the host to forward packets under any circumstances. The same set of instructions should apply to most UNIX systems, but the exact file names and locations may vary.

Also included are instructions for changing the *ipforwarding* variable in the binary file used to build new kernels. This keeps IP forwarding from re-occurring should a new kernel be built and installed at some future time.

You must be a super user with root privileges to run the following commands. Be very careful to type these commands correctly, as you will be changing the UNIX kernel. If your system is a recent implementation based on BSD 4.3 (such as SunOS 4.0 or higher), then you may ignore these instructions.

In the following example, be sure to use the single quote character (’) as shown.

Example:

To modify the **ipforwarding** kernel variable, execute the following command on your SunOS system. (Please note that a capital ‘‘D’’ is being used in this command.)

echo ’ipforwarding?D’ | adb /vmunix
Adb should respond with
‘‘*_ipforwarding 1*’’.

If the value is zero, then *ipforwarding* is already shut off.

If it is one, then do the following. (Please note that a capital ’’W‘‘ is being used, immediately followed by a zero in this command.)

echo ’ipforwarding?W0’ | adb -w /vmunix

This writes the new value into the /vmunix file. You will have to reboot the host for this change to take effect.

If you ever rebuild the kernel on your workstation the *ipforwarding* flag will be reset to its initial state due to using the original binary files shipped with your workstation. To prevent this from happening in the event that the kernel is rebuilt at some time in the future, you need to modify the kernel binary image that contains the *ipforwarding* code.

In the case of a Sun server the kernel files are located in /sys/<sun2,3,or 4>/OBJ. The file in question is ip_input.o. You can set the *ipforwarding* flag to zero in this file by using the ‘‘cd’’ command to move to the appropriate OBJ directory, becoming root and executing the following string:

echo ’ipforwarding?W0’ | adb -w ip_input.o

This writes the value into the ip_input.o file so that if and when a kernel is rebuilt using this file, the *ipforwarding* flag will be zero.

If you ever plan to use your Sun as a gateway machine, setting *ipforwarding* off as shown above will keep the gateway software from functioning properly. As it happens, Sun systems do not make effective gateways for UTnet, due to the inability of the embedded gateway code to support the special configuration required to make routing work effectively on a combination bridge and router backbone such as UTnet. Be warned that all versions of SunOS 4.0 up to SunOS 4.0.3 contain a serious bug in the gateway software and systems running this software should *never* be used as gateway machines.