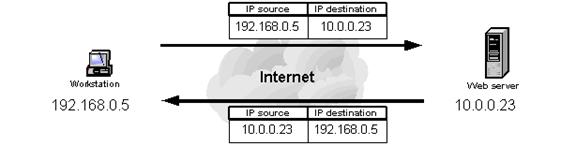
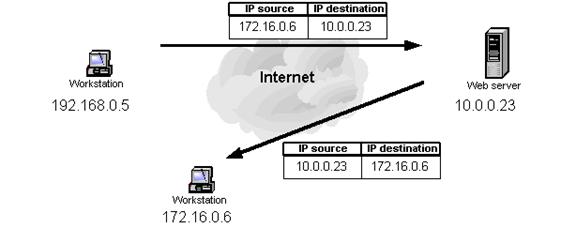
TCP/IP protocol suite which is a part of universally agreed upon set of protocols, is used to specify how data is transmitted across packet switched networks over the Internet. It uses numeric identifiers called IP addresses to uniquely identify computers on a network. Network communications like emails, file transfers, or web page requests all require the use of valid source and destination IP addresses. The basic unit of data transfer in a packet switched network is called an IP datagram packet. An IP datagram carries enough information about the network to get forwarded to its destination*.* Layers above IP use the source address in an incoming packet to identify the sender and as IP makes no effort to validate whether the source address in the packet generated by a node is actually the source address of the node, one can easily spoof the source address. This article focuses on the various types of attacks that involve IP spoofing on networks along with the techniques and approaches that experts in the field suggest to contend with this problem.

***What is IP Spoofing?***

IP spoofing, also known as IP address forgery or a host file hijack, is a [hijacking](http://searchsecurity.techtarget.com/definition/hijacking) technique in which a [cracker](http://searchsecurity.techtarget.com/definition/cracker) masquerades as a trusted [host](http://searchcio-midmarket.techtarget.com/definition/host) to conceal his identity, [spoof](http://searchsecurity.techtarget.com/definition/spoof) a Web site, hijack browsers, or gain access to a network. It occurs when the attacker determines and uses an IP address of a network, computer, or network component without being authorized to do so. A successful attack allows the attacker to operate as if the attacker is the entity normally identified by that spoofed IP address. This situation comes into play only if an administrator has done both of the following:

* Configured connections that support only Transmission Control Protocol (TCP) (which is not recommended, because TCP communications are unencrypted).
* Marked the IP addresses of those connections as trusted hosts.

When IP spoofing is used to hijack a browser, a visitor who types in the [URL](http://searchnetworking.techtarget.com/definition/URL)(Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the IRS Web site, then any Internet user who typed in the URL www.irs.gov would see spoofed content created by the hijacker. If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password or SSN, or install [malware](http://searchmidmarketsecurity.techtarget.com/definition/malware) . The hijacker would also be able to take control of a compromised computer to use it as part of a [zombie army](http://searchsecurity.techtarget.com/definition/botnet) in order to send out spam.  
  
 

**Valid source IP address** **Spoofed Source IP address**

***How it can be done?***

The IP stack in the operating system takes care of the header for the IP datagram. However, you can override this function by inserting a custom header and informing the operating system that the packet does not need any headers. You can use raw sockets in UNIX-like systems to send spoofed IP datagrams, and you can use packet drivers such as WinPcap on Windows. Some socket programming knowledge is enough to write a program for generating crafted IP packets. You can insert any kind of header, so, for example, you can also create Transmission Control Protocol(TCP) headers. If you do not want to program or have no knowledge of programming, you can use tools such as hping, sendip,and others that are available for free on the Internet, with very detailed documentation to craft any kind of packet. Most of the time, you can send a spoofed address IP packet with just a one-line command. You can spoof at various network layers; for example, you can use Address Resolution Protocol(ARP) spoofing to divert the traffic intended for one station to someone else. The Simple Mail Transfer Protocol(SMTP) is also a target for spoofing; because SMTP does not verify the sender's address, you can send any e-mail to anybody pretending to be someone else.

***Why Spoof the IP Source Address?***

 You can use IP spoofing for several purposes; for some scenarios an attacker might want to inspect the response from the target victim (called "nonblind spoofing"), whereas in other cases the attacker might not care (blind spoofing). Following are the reasons to spoof an IP packet :

<http://people.scs.carleton.ca/~dlwhyte/whytepapers/ipspoof.htm>

<http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html>

<http://en.wikipedia.org/wiki/IP_address_spoofing>

http://searchsecurity.techtarget.com/definition/IP-spoofing