

# Abnormal IP Packets

*Karen Kent Frederick* 2000-10-13

## Introduction

This article, a discussion of the characteristics of abnormal Internet Protocol (IP) packets, is the first in a series of tutorials that are intended to educate intrusion detection system administrators about IP. As the use of network intrusion detection systems becomes more widespread, system administrators must learn how to use them effectively. Unfortunately, many admins do not have a thorough knowledge of IP. So even though an IDS may produce alerts about particular scans and attacks, an admin may not understand what the alerts mean.

IP protocol standards are defined in the RFC (Request for Comments) documents, which are available at <http://www.ietf.org/rfc.html>. For the sake of this article, we define abnormal packets as those which violate those standards. Abnormal packets may be generated through benign means, such as a malfunctioning router, but they are usually specially crafted by attackers. The abnormality is often introduced into the packet purposely so that the packet may avoid being blocked by a firewall or intrusion detection system. In other cases, abnormal packets are used to attempt to crash systems. A great place to see real examples of abnormal packets is the SANS Institute's [Global Incident Analysis Center](#).

## IP Protocol Types

There are many different types of IP protocols. You are probably familiar with at least three of them: the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP) and the Internet Control Message Protocol (ICMP). There are dozens of other IP protocols; examples that you may know include routing protocols such as IGRP, EIGRP and OSPF. Each IP protocol type has its own value, called an Internet Protocol number. These are important to know because some systems log packets by the IP number, not the corresponding abbreviation. In this article, we will review some characteristics of the most commonly seen types, which are type 1 (ICMP), type 6 (TCP) and type 17 (UDP). A list of all of the IP numbers is available at <ftp://ftp.isi.edu/in-notes/iana/assignments/protocol-numbers>.

RFC 791 described a four bit field that was to be used to identify the underlying internetworking protocol of a packet. The Internet Protocol that we are familiar with is version number 4. The new version of IP, which will be deployed in the coming years, is version number 6. Normally,

you should never see any packet with a version number other than 4, but you may occasionally come across one. If you see a packet with a version other than 4, you can be pretty sure that it is crafted. For more information, visit <http://www.isi.edu/in-notes/iana/assignments/version-numbers>.

## IP Addresses

Certain IP addresses have been specially designated by the Internet Assigned Numbers Authority (IANA) as reserved for internal network use only, not for Internet use. The reserved address ranges are: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 and 192.168.0.0 - 192.168.255.255. (Read RFC 1918, "Address Allocation for Private Internets", at <http://www.isi.edu/in-notes/rfc1918.txt> for more information.) Although these addresses should never be seen over the Internet, they are. Sometimes this is caused by equipment which has been misconfigured; for example, a firewall may accidentally be allowing internal address to "leak" onto the Internet. Also, computers that unsuccessfully attempt to get a valid IP address through DHCP typically are assigned addresses on the 169.254 subnet. Another reason for seeing these addresses on the Internet is that attackers are creating crafted packets with false IP addresses. This technique is better known as IP spoofing.

The main reason for performing IP spoofing is to make it harder for an attack to be traced back to its real IP address. Attackers may use addresses in the reserved address ranges listed above; more commonly, they use regular addresses which belong to someone else. So if your system is attacked, you may trace it back to an innocent third party. Another type of IP spoofing attack, called a Land attack, uses packets with the source and destination address set to the same value. Packets should always have different source and destination addresses, so your network devices should reject any packet where those values are the same.

In order to protect your network from IP spoofing generated by attackers on the Internet or on your own network, you should only permit incoming packets with a source address outside your network's range, and outgoing packets with a source address in your network's range. Also, packets that have a source or destination address in one of the ranges previously mentioned should not be permitted through Internet-based devices.

## TCP Packets

TCP is a connection-oriented protocol; it uses various flags to indicate that a connection is being

started or ended, or that the data carries a high priority. Many attacks are based on altering the TCP flags. Certain illegal combinations of TCP flags may be able to help packets avoid detection by firewalls or intrusion detection systems; other illegal combinations may be used to crash operating systems.

The functional specification for TCP is defined in [RFC 793](#). This RFC and others define how systems should respond to legitimate packets, but they don't explain how systems should handle illegal combinations of flags. Consequently, different operating systems respond differently to illegal flag combinations. Attackers can exploit this to determine what operating system a device is using.

At least one of these six flags must be set in each TCP packet; each flag corresponds to a particular bit in the TCP header. The six flags are:

- SYN (Synchronization) - Initiate a TCP connection.
- ACK (Acknowledgment) - Indicates that the value in the acknowledgment number field is valid.
- FIN (Finish) - Gracefully end a TCP connection.
- RST (Reset) - Immediately end a TCP connection.
- PSH (Push) - Tells the receiver to pass on the data as soon as possible.
- URG (Urgent) - Indicates that the urgent pointer is valid; often caused by an interrupt.

Before reviewing abnormal flag combinations, let's look at the normal ones:

- SYN, SYN ACK, and ACK are used during the three-way handshake which establishes a TCP connection.
- Except for the initial SYN packet, every packet in a connection must have the ACK bit set.
- FIN ACK and ACK are used during the graceful teardown of an existing connection. PSH FIN ACK may also be seen at the beginning of a graceful teardown.
- RST or RST ACK can be used to immediately terminate an existing connection.
- Packets during the "conversation" portion of the connection (after the three-way handshake but before the teardown or termination) contain just an ACK by default. Optionally, they may also contain PSH and/or URG.

Packets with any other flag combination can be classified as abnormal. Here are some of the

most commonly occurring ones:

- SYN FIN is probably the best known illegal combination. Remember that SYN is used to start a connection, while FIN is used to end an existing connection. It is nonsensical to perform both actions at the same time. Many scanning tools use SYN FIN packets, because many intrusion detection systems did not catch these in the past, although most do so now. You can safely assume that any SYN FIN packets you see are malicious.
- SYN FIN PSH, SYN FIN RST, SYN FIN RST PSH, and other variants on SYN FIN also exist. These packets may be used by attackers who are aware that intrusion detection systems may be looking for packets with just the SYN and FIN bits set, not additional bits set. Again, these are clearly malicious.
- Packets should never contain just a FIN flag. FIN packets are frequently used for port scans, network mapping and other stealth activities.
- Some packets have absolutely no flags set at all; these are referred to as "null" packets. It is illegal to have a packet with no flags set.

Besides the six flag bits described here, TCP packets have two additional bits which are reserved for future use. These are commonly referred to as the "reserved bits". Any packet which has either or both of the reserved bits activated is almost certainly crafted.

There are several other characteristics of TCP traffic where abnormalities may be seen:

- Packets should never have a source or destination port set to 0.
- The acknowledgment number should never be set to 0 when the ACK flag is set.
- A SYN only packet, which should only occur when a new connection is being initiated, should not contain any data.
- Packets should not use a destination address that is a broadcast address, usually ending in .0 or .255. (You may not be familiar with .0 as a broadcast address; it was an older style of broadcast.) Broadcasts are normally not performed using TCP.

Many of the tools used by attackers to scan and probe your networks are based on the use of abnormal TCP packets. A large percentage of alerts detected by intrusion detection systems involve these types of packets, so it is critical to be able to identify them and understand their purpose. By configuring your intrusion detection system to alert on all abnormal TCP packets, you may catch malicious activity that you were not previously seeing.

## UDP Packets

Unlike TCP, UDP is a connectionless protocol. UDP does not have the flag and reserved bits that TCP does. However, both TCP and UDP rely on source and destination ports. Like TCP, packets, UDP packets should never have a source or destination port set to 0. UDP packets can also be fragmented maliciously; see the "Fragmentation" section below for more information on this technique.

## ICMP Packets

ICMP is used to pass an error message between two hosts or a host and a network device such as a router. Since UDP and IP are connectionless protocols, they rely on ICMP to transmit error messages on their behalf. To avoid potential error message loops, responses are never sent to ICMP error messages. ICMP has no port numbers; it uses ICMP message types and codes instead. Another noteworthy characteristic of ICMP is that it supports broadcast traffic. Since ICMP packets are not very complicated, there are not that many ways that they can be made abnormal.

One type of ICMP message that is used maliciously is a redirect. ICMP redirect messages are intended to be sent from a router to a host, in order to inform that host that a different router is more optimal than it is when contacting a particular destination address. Some attacks such as WinFreeze use false ICMP redirect messages to attempt to convince a host to use itself as the optimal router. Obviously, any packet which tells a device to route everything to itself should be considered highly abnormal.

Most ICMP packets are composed of a small header and payload; for example, most ICMP echo request packets have an 8-byte header and a 56-byte payload. ICMP packets that are significantly larger than normal should be considered suspicious. Also, some ICMP types, such as echo requests, should not be carrying any data. Some malicious applications, including various distributed denial of service programs and tunneling programs, use ICMP packets as "containers" that hide other traffic. So an ICMP echo reply might actually contain a completely different IP protocol within its data, for example. If you monitor your systems for large ICMP packets or for packets of specific ICMP types that should not contain data but do, you should be able to detect this type of traffic.

## Fragmentation

When an IP packet is too large to be transmitted as one entity, it must be split into two or more smaller pieces that can be sent across networks. Each piece of a packet is referred to as a fragment. Fragmentation occurs for all of the protocols we are discussing - TCP, UDP and ICMP - although it occurs most frequently for TCP. However, attackers can create artificially fragmented packets. In some cases, this is done in order to attempt to crash systems; in other cases, it is done to circumvent firewall rules or avoid intrusion detection systems. Some firewalls and intrusion detection systems do not perform packet reassembly, so they can only consider the properties of each individual fragment.

One type of malicious fragmentation involves fragments that have illegal offsets. An offset value indicates where a fragment's data should be placed in a reassembled packet. The first fragment appears to be normal, except that it is usually very small. The second fragment has a data offset value which is less than the length of the data in the first packet. So if the first fragment had 24 bytes of data, the second fragment might claim to have an offset of 20 bytes. This would mean that the data in the second fragment would overwrite the last four bytes of the data from the first fragment. If the fragmented packet was TCP, then the first fragment would contain the TCP header. The purpose of the offset value of the second fragment would be to overwrite part of the first packet's TCP header, such as the destination port number, when the packet is reassembled at the destination. So an attacker could send a fragmented packet through your firewall to your web server on port 80, but when the web server reassembles the fragments, the final packet could actually go to a completely different port.

The same type of attack can be used to crash systems. In some older operating systems, when the receiving host attempts to rebuild such a packet, it calculates a negative length for the second fragment. This value is passed to a function which should do a copy from memory. Unfortunately, the memory copy cannot handle a negative number, so it thinks that the small negative number is actually an enormous positive number.

A second type of attack involving fragments is known as the tiny fragment attack. Two TCP fragments are created. The first fragment is so small that it does not even include the full TCP header, particularly the destination port number. The second fragment contains the remainder of the TCP header, including the port number. Some firewalls and intrusion detection systems may let one or both fragments pass through, particularly if they do not perform packet reassembly.

Another type of attack involves sending a fragmented, abnormally large packet. The attacker hopes that when the receiving host receives the fragments, it will crash while attempting to reassemble the packet, since the whole packet has an illegal length. (In case you are not aware, packets have minimum and maximum lengths.) The best-known example of this attack type is the infamous Ping of Death attack. It creates an ICMP echo request packet which is larger than the maximum packet size of 65,535 bytes.

Some attacks use packets that are not illegal but are extremely suspicious. For example, suppose that you receive a fragmented TCP packet that only has the SYN flag set. Since a SYN-only packet is not allowed to carry any data, it should not be large enough to require fragmentation. If you encounter such a packet, treat it with great suspicion.

So how can you protect your network against fragmentation attacks? As mentioned previously, you should implement firewalls and intrusion detection systems that can perform packet reassembly. You should also configure your intrusion detection system to alert on any extremely small fragments other than the final fragment in a packet. Under normal circumstances, you should not be seeing small initial fragments; these are normally malicious in nature. Also, remember to keep your systems current with all patches and updates.

## Conclusion

Anyone who is involved with intrusion detection should have a solid knowledge of what normal and abnormal IP traffic is. It is not uncommon for the administrator of an intrusion detection system to get great alerts from the IDS but not understand what they really mean. Hopefully, by studying more about IP and thinking about the concepts presented in this article, you can better interpret alerts and analyze what is really happening on your network.

*Karen Kent Frederick is a senior security engineer for NFR Security. Karen has a B.S. in Computer Science and is completing her Master's thesis in intrusion detection through the University of Idaho's Engineering Outreach program. She holds several certifications, including Microsoft Certified Systems Engineer + Internet, Check Point Certified Security Administrator, and GIAC Certified Intrusion Analyst. Karen is one of the authors and editors of "Intrusion Signatures and Analysis", a book on intrusion detection that will be published in January 2001.*

## Relevant Links

[Subscribe to the FOCUS-IDS Mailing List](#)

*SecurityFocus*

[Privacy Statement](#)

Copyright 2006, SecurityFocus