Prevention of ICMP Jumbo Frames on the SG200/300 Series Managed Switches

Objective

The objective of this article is to explain why SG200 and SG300 series switches prevent some of the ICMP jumbo frames and allow other jumbo frames to pass over the Switch. This article shows what some of the problems are due to ICMP jumbo frames. The article also explains what a Denial of Service (DoS) attack is and how it relates to ICMP jumbo frames.

Applicable Devices

- SG200
- SG300

ICMP Jumbo frames Over the Switch

The following explains what jumbo frames are and why ICMP jumbo frames are not allowed on SG200 and SG300 series switches.

Jumbo Frames

The Gigabit Ethernet switch (SG200 and SG300 Series) and Fast Ethernet switch (SF200 series switches) support jumbo frames. The **Jumbo Frames** are extended Ethernet frames that range in size from the standard 1,518 bytes up to 9,000 bytes. Thus the jumbo frames increase the data transfer speed by carrying more data per frame, reducing the overhead from headers.

Internet Control Message Protocol (ICMP)

ICMP is a network layer protocol that is a part of the Internet Protocol suite which generates ICMP messages in response to errors in the IP datagram or for diagnostic or routing purposes. ICMP errors are always reported to the original source IP address of the originating datagram. Although this protocol is very important for ensuring correct data distribution, it can be exploited by malicious users for conducting different Denial of Service (DoS) attacks.

DoS attacks make network and server resources unavailable or unresponsive to legitimate users through flooding networks with false traffic. DoS attacks by brute force consume the server and network bandwidth by flooding the server with overwhelming traffic. The following are common types of DoS attacks using ICMP.

- ICMP Ping Flood Attack — In an ICMP Ping Flood attack, the attack sends huge numbers of ping packets to the target system usually through using the ping command from the host. In this way the attacked system can not respond to legitimate traffic.

- ICMP Smurf Attack — An ICMP Smurf Attack floods the victim machine with spoofed ping packets. These are modified packets which contain a spoofed IP address of the target victim. This causes a broadcast of the misinformation to all hosts in the local network. All of

these hosts respond with a reply to the target system, which is then saturated with those replies.If there are many hosts in used networks, the victim will be effectively spoofed by a large amount of traffic.

Note: IP Spoofing refers to an IP packet with a forged source IP address, with the purpose of concealing the information of the sender.

• Ping of Death — In a ping of death attack, the attacker sends the victim an ICMP echo request packet that is larger than the maximum IP packet size of 65.536 bytes. Since the received ICMP echo request packet is larger than the normal IP packet size, it must be fragmented. As a result of this, the victim is unable to reassemble the packets, so the OS crashes or reboots.

• ICMP Nuke Attack — In this type of attack, nukes are sent to the victim through an ICMP packet with destination unreachable messages that are type 3. The result of this attack is that the target system breaks communications with existing connections.

In SG200 and SG300 series switches the Denial of Service Prevention enables network managers to configure the blocking of certain ICMP packets. By default some of the ICMP jumbo frames are blocked because many network attacks such as DoS utilize ICMP, so for the security reasons the firewalls of these switches block ICMP jumbo frames. This results in the necessary ICMP fragmentation and the DF set message not reaching the sender. The sender thus gets no information to send its packets at a smaller size, nor does it get a TCP confirmation that its packets were successful. Subsequently, the sender then continuously resends the frame at the same large size, but it never reaches the destination, resulting in a condition known as a "black hole."

Use the web configuration utility to configure jumbo frames, and choose **Port management > Port Settings** and choose **Security > Denial of Service Prevention > Security Suite Settings** to configure DoS prevention.