Lantech®
Pioneering Industrial and IP Networks

White Paper

Lantech Solution to Prevent

DoS / DDoS Attacks

Version 1.0
Feb, 2023

https://www.lantechcom.tw | info@lantechcom.tw

A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack uses fake user traffic to occupy network resources and make a website or resource unavailable. Both types of attacks overload servers or web applications with the goal of disrupting services on the web.

What are DoS / DDoS attacks?

DoS (Denial of Service) Attacks

The common Dos attack is where hackers use a relatively powerful single computer to attack a target IP, this is a one-to-one attack (DDoS is a many-to-one attack). DoS sends a large number of meaningless network messages to the target IP in the form of message flooding, exhausting system or network resources and making the service unable to operate normally.

DDoS (Distributed Denial of Service) Attacks

DDoS has evolved from DoS. DDoS attacks allow hackers to take control of multiple malware-infected computers or other devices such as IoT devices, this is becoming what is often heard as a "zombie computer". As the source of attack traffic, these zombie computers launch a "denial of service" attack on a specific target IP, introducing a large amount of network traffic, overwhelming the server or network, causing the host to temporarily interrupt or stop the service.

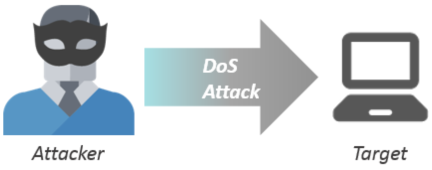

Figure 1 – Denial-of-service (DoS) attacks

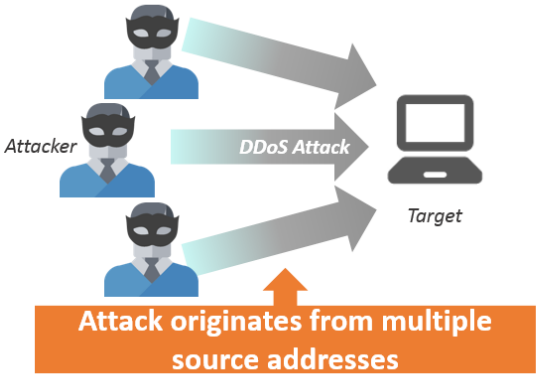

Figure 2 – Distributed denial-of-service (DDoS) attack

Lantech solutions to prevent DoS / DDoS attacks

Lantech OS3/OS4 switches adjust the access rules, strengthening the screening mechanism, limits and blocks abnormal IP addresses or abnormal request packets, this reduces the possibility of a large amount of invalid data occupying bandwidth or consuming resources, this then achieves the effect of blocking DoS/DDoS attacks.

Figure 3 – Check the suspicious packets	*Figure 4 – Check the suspicious traffic flow and connection*

Lantech OS3/OS4 Switches' Mechanisms for Suspicious Packets DoS/DDoS Attacks

- ICMP Fragment Protection
- IP Packet Fragment Protection
- TCP Null Scan Protection
- TCP over MAC Multicast / Broadcast Protection
- TCP Flags with FIN-URG-PSH Protection
- TCP Flags with SYN-RST Protection
- TCP Flags with SYN-FIN Protection
- TCP Flags with FIN-RST Protection
- TCP/UDP port is zero Protection
- ARP MAC SA Mismatch Protection
- FIN Scan (OS4)

Lantech OS3/OS4 Switches' Mechanisms for Network DoS/DDoS Attacks

- SYN Flood Protection
- ICMP Flood Protection
- UDP Flood Protection
- DHCP Snooping
- Port Security

- Rogue DHCP Server Attack Protection
- Dynamic ARP Inspection (DAI)
- IP Source Guard
- TCP/UDP Port Scanning Protection
- Smurf/Fraggle Attack Protection
- ARP Flood
- TCP Blat (OS4)
- UDP Blat (OS4)
- TCP-SYN (SPORT<1024) (OS4)

Conclusion

The reason why DDoS defense is difficult is that DDoS "attacks" will be packaged with seemingly normal "needs", and the source of the attack is also difficult to trace. However, the following four aspects can still be used to strengthen the system's DDoS defense:

1. Implement periodic information security testing.
2. Regular adjustments of the rules of the road for protective equipment
3. Improve the equipment performance and specifications of the service system
4. Adopt mechanisms with DDoS defense or DDoS mitigation

Using Lantech OS3/OS4 switches with DDoS attack protection mechanisms can not only protect the switch itself, but also protect the backend devices connected to the switch, such as servers, cameras, and wireless APs.

Comparison of Lantech OS3/OS4 Switches and Other Brands

Regarding the Protection of DDoS/DoS Attacks

Features	Lantech OS3	Lantech OS4	Brand M	Brand A
ICMP Fragment Protection	✓	✓	✗	✓
Large ICMP packet size protection	✗	✗	✗	✓
TCP SYN Fragment protection	✗	✗	✗	✗
IP Packet Fragment protection	✓	✓	✗	✓
Bad IP Option protection	✗	✗	✗	✗
Unknown Protocol protection	✗	✗	✗	✗
TCP Null Scan protection	✓	✓	✓	✓
TCP over MAC Multicast/Broadcast protection	✓	✓	✗	✗
TCP Flags with FIN-URG-PSH protection	✓	✓	✓	✓
TCP Flag with SYN-RST protection	✓	✓	✓	✓
TCP Flag with SYN-FIN protection	✓	✓	✓	✓
TCP Flag with FIN-RST protection	✓	✓	✗	✗
TCP/UDP port is 0 protection	✓	✓	✗	✗
ARP MAC SA Mismatch protection	✓	✓	✗	✗
SYN flood protection	✓	✓	✓	✗
ICMP Flood protection	✓	✓	✓	✓
UDP Flood protection	✓	✓	✗	✗
DHCP Snooping	✓	✓	✓	✓
Port Security	✓	✓	✗	✗
Rogue DHCP server attack protection	✓	✓	✗	✗
Dynamic ARP Inspection (DAI)	✓	✓	✗	✗
IP Source Guard	✓	✓	✗	✗
TCP/UDP port scanning protection	✓	✓	✗	✗
Smurf/Fraggle attack protection	✓	✓	✗	✓
ARP Flood	✓	✓	✓	✗
FIN Scan	✗	✓	✓	✗
DMAC=SMAC	✗	✗	✗	✓
TCP Blat	✗	✓	✗	✓
UDP Blat	✗	✓	✗	✓
TCP-SYN (SPORT<1024)	✗	✓	✗	✓

About Lantech

Lantech Communications Global, Inc. is an IRIS, IEC 62443-4-1 & ITxPT certified manufacturer of Ethernet products focused on the transportation markets, bus, train, trackside, ITS, smart city and many more applications. Our range of onboard EN50155 & E-Marked Ethernet switches & wireless/ LTE routers offer cutting edge design and functionality. We continue to work with our key customers in creating further enhancements & developments in on board passenger information, video security, trackside data communications by providing rugged 10GbE, PoE managed Ethernet switches, LTE/Wi-Fi routers in line with ITxPT and E-Marked certifications for various applications and critical solutions.