Reference: Overview of Incident

Securities Company
(Merrill Lynch Japan Securities)

Order system

Virtual Server ① (Address A : Port B)

Virtual Server ② (Address A : Port B)

Two virtual servers with the same IP address and port numbers attempted to establish a TCP connection, resulting in a discrepancy in the management number leading to a massive number of retransmission messages being sent.

Message Transmission Image

Virtual Server — GW server

Mgmt. # discrepancy

Normal process with VS 1

Large volume of msgs from VS 2

Merge

①Lg # msgs →High stress

②Suspension

Securities Company

Order system

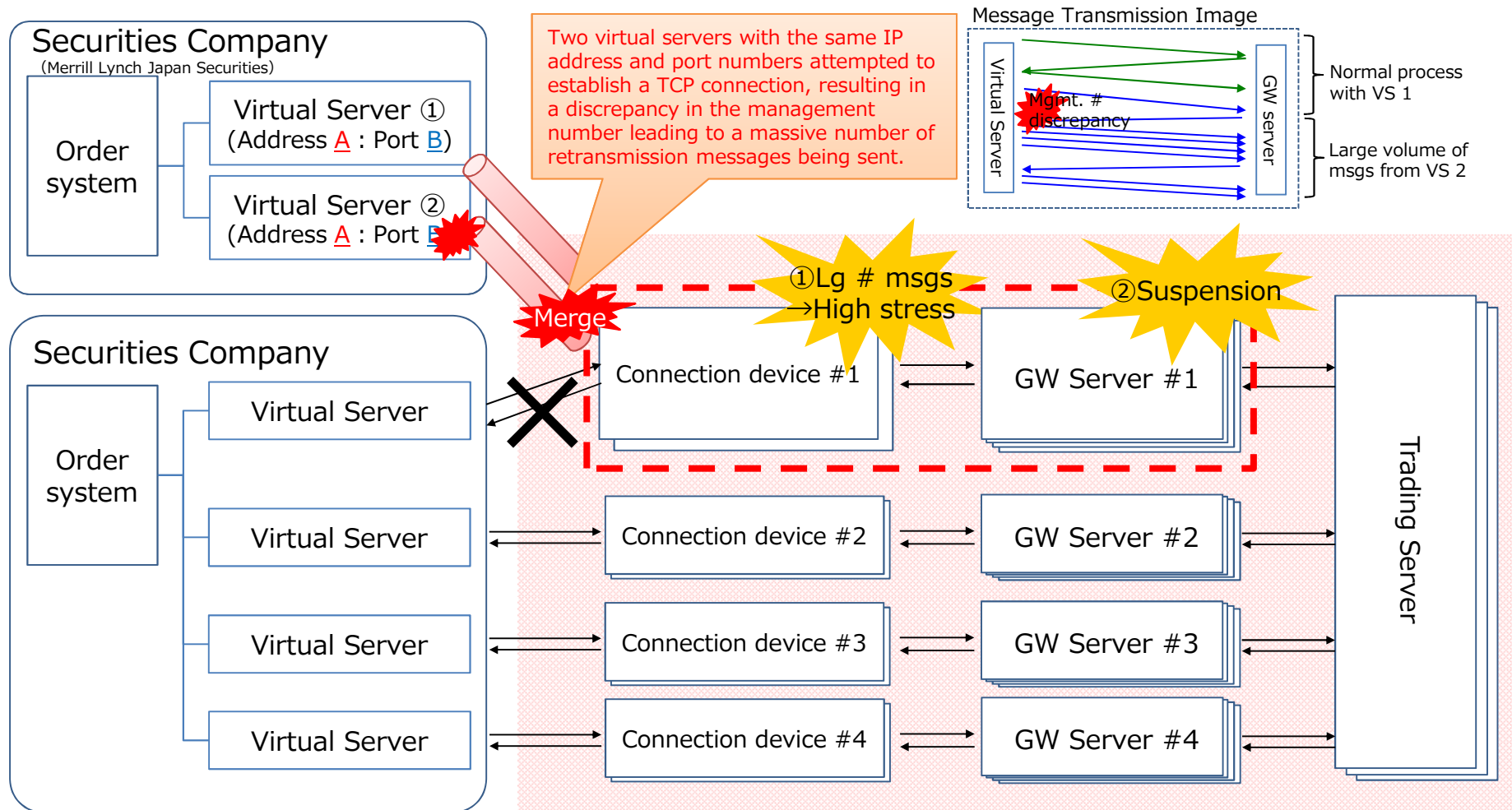| Virtual Server | Connection device #1 | GW Server #1 | Trading Server |
Virtual Server	Connection device #2	GW Server #2	
Virtual Server	Connection device #3	GW Server #3	
Virtual Server	Connection device #4	GW Server #4	

- Securities companies use virtual servers – connection points to the arrowhead system – to connect to arrowhead gateway servers ("GW servers") and send order messages to trading servers which process trading.

【Behavior on the day of the incident】

- Virtual servers that were assigned the same IP address and port number were activated simultaneously, which resulted in a discrepancy in the TCP connection management number. This triggered a massive number of retransmission messages to be sent to the system in a short period of time.
- Connection device #1 experienced heavy stress, which resulted in the system suspending the function of all GW servers connected to that connection device to maintain stability.
- The virtual servers connected to the GW servers under connection device #1 were unable to connect to arrowhead, and orders were unable to be place on that connection route.