Case Reference	R/E/I/128
Title	SingNet's Service Difficulty Incident on 3 December 2016 **("Incident")**
Case Opened	3 December 2016
Case Closed	18 August 2017
Complainant	IMDA initiated this proceeding pursuant to the Code of Practice for Telecommunication Service Resiliency 2016
Respondent	SingNet Pte Ltd **("SingNet")**
Case Summary	On 3 December 2016, a disruption to SingNet's fibre broadband services affected approximately 90% of its active fibre broadband subscribers nationwide. Subscriber services were progressively restored during the Incident which lasted from 0846hrs on 3 December 2016 to 0825hrs on 4 December 2016. The affected subscribers were unable to obtain IP addresses and access the Internet services during the Incident. The Incident was caused by an overloading of the Central Processing Units **("CPU")** of SingNet's Dynamic Host Control Protocol **("DHCP")** servers, which resulted in the DHCP servers being unable to process requests for IP addresses.
IMDA's Determination	IMDA's investigation revealed that following SingNet's enabling of IPv6 traffic at its DHCP servers in June 2016, there had been a steady increase in the CPU utilisation load of its DHCP servers, and the utilisation level reached 80%-90% just before the occurrence of the Incident. On 3 December 2016, when SingNet carried out a planned maintenance to install kernel/security patches on the DHCP servers, it resulted in a surge of DHCP traffic, and tipped the CPU loads of the DHCP servers to 100%. This led to a congestion in the processing of requests for IP addresses and resulted in the Incident. IMDA found that the high CPU load in the DHCP servers leading up to the Incident was caused by the sub-optimal processing of IPv6 traffic by the DHCP servers' software. It was a software design limitation that SingNet and its vendor were not aware of. Nevertheless, IMDA determined that SingNet should have noted the warning signs provided by the high CPU utilisation level of 80%-90%, and had sufficient time since June 2016 to take measures to reduce the load levels. SingNet should also have exercised greater care and diligence before it proceeded to install the security/kernel patches on its DHCP servers in December 2016, in view of the high CPU loads. In particular, in anticipation of the surge in DHCP traffic during the planned maintenance, SingNet should have reviewed and taken prompt actions to address the high CPU loads of the DHCP servers, such as increasing

	the DHCP's IP lease time temporarily, or increasing the capacity of the DHCP servers, before it proceeded to install the security/kernel patches. Accordingly, IMDA determined that SingNet had not established to the satisfaction of IMDA that the occurrence of the Incident was not within its control and had occasioned through no fault on its part. While SingNet or its vendor might not have been aware of the IPv6 design limitation in the DHCP server software, the Incident was largely caused by SingNet's failure to take prompt action to address the increasing CPU utilisation levels prior to the Incident, and SingNet not acting prudently in deciding to proceed with the installation of the kernel/security patches on the DHCP servers, despite the high CPU loads and knowing that there would likely be a spike in DHCP traffic upon rebooting of the DHCP servers. The Incident was severe as it affected approximately 90% of SingNet's fibre broadband subscribers nationwide. Subscriber services were progressively restored during the Incident which lasted for 23 hours and 39 minutes. Nevertheless, IMDA noted that SingNet had proactively and promptly offered compensation to its subscribers affected by the Incident, in the form of mobile data charges waiver and monthly subscription fee discount during the incident to mitigate the impact. It had also since taken measures to prevent a recurrence of the Incident. These include a) upgrading its existing DHCP servers; b) setting up a separate standalone IPv6 DHCP server; and c) conducting an end-to-end review of its broadband network architecture, vendor management of critical platforms, and its escalation process to improve the resiliency of the network. Finally, IMDA took into consideration the full co-operation rendered by SingNet to IMDA in its investigation, which allowed IMDA to complete its investigation swiftly. Taking all factors into consideration, IMDA decided to impose a financial penalty of $500,000 on SingNet for the Incident.