Received: 27 July 2018 | Revised: 21 December 2018 | Accepted: 11 January 2019

DOI: 10.4218/etrij.2018-0309

ORIGINAL ARTICLE

WILEY ETRI Journal

FDVRRP: Router implementation for fast detection and high availability in network failure cases

Changsik Lee | **Suncheul Kim** | **Hoyong Ryu**

Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea

Correspondence
Changsik Lee, Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea.
Email: cslee2624@etri.re.kr

Funding information
ICT R&D program of MSIP/IITP, Republic of Korea, Grant/Award Number: 2012-2-00210.

High availability and reliability have been considered promising requirements for the support of seamless network services such as real-time video streaming, gaming, and virtual and augmented reality. Increased availability can be achieved within a local area network with the use of the virtual router redundancy protocol that utilizes backup routers to provide a backup path in the case of a master router failure. However, the network may still lose a large number of packets during a failover owing to a late failure detections and lazy responses. To achieve an efficient failover, we propose the implementation of fast detection with virtual router redundancy protocol (FDVRRP) in which the backup router quickly detects a link failure and immediately serves as the master router. We implemented the FDVRRP using open neutralized network operating system (OpenN2OS), which is an open-source-based network operating system. Based on the failover performance test of OpenN2OS, we verified that the FDVRRP exhibits a very fast failure detection and a failover with low-overhead packets.

KEYWORDS
failover, fast detection, high availability, virtual router redundancy protocol

1 | INTRODUCTION

Following the deployment of real-time services such as video streaming, gaming, and virtual and augmented reality, current computer networks are confronted with increasing demands highly available, reliable, and seamless network service provisions. To meet these requirements, there have been many studies on data transmission techniques, such as data compression [1,2], encryption [3,4], and transmission methods [5,6]. However, these techniques cannot be used if we are unable to cope with a network link down or equipment failure (i.e. L2 switches or L3 routers). For this reason, we need to focus on how to handle a network failure in a more efficient manner.

In traditional computer networks with a single gateway system, network devices can communicate with an external network only through a single gateway. In this single gateway system, however, a single point of failure (SPOF) problem may occur, as shown in Figure 1. If a gateway router fails, network devices in a local area network (LAN) cannot communicate with an external network. To tackle this SPOF problem, we can utilize a router redundancy method [7]. Router redundancy refers to the case where extra routers exist to provide a backup path in the case of a primary router failure. If a router fails, the routing functionalities should be seamlessly shifted from one router to another without any disruption of the internal network. A significant challenge has also been the allocation of redundant routers—when these routers exist—to achieve high availability [8].

Currently, there are three main router redundancy protocols that can be implemented in a router: (a) a hot standby router protocol (HSRP) [9], (b) a gateway load balancing

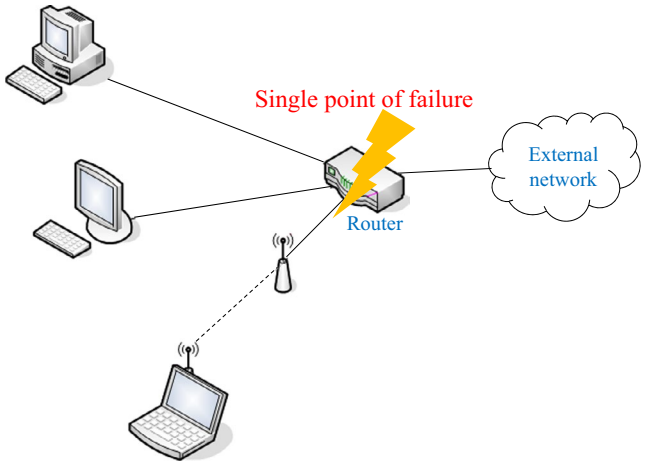


FIGURE 1 SPOF problem

protocol (GLBP), and (c) a virtual router redundancy protocol (VRRP) [10–14]. All these protocols have their own specifications and have a similar mechanism. However, both HSRP and GLBP are Cisco proprietary software and are inherently closed source, whereas VRRP is an open standard created by the Internet Engineering Task Force (IETF). By adopting the open standard protocol instead of commercial software, network enterprises can reduce the considerable license fee and maintenance costs and achieve increased flexibility. In an effort to develop an open networking framework independent of specific network vendors, we utilized the open-source VRRP. Many studies have aimed at increasing the fault-tolerance responses of networks by either adopting these router redundancy solutions [15,16], or the fast reroute (FRR) technology used in IP/MPLS networks. Additionally, the VRRP mechanism has been adopted as a solution for fault-tolerance issues for networking (SDN) controllers defined based on software [17].

According to the VRRP specifications, it takes more than 3 s for the backup router to detect a failure at the master router. However, this delay still makes it difficult to support seamless and real-time network services. To cope with a network failure more efficiently, we need a mechanism that achieves the prompt detection of failures in the path between the VRRP routers. To meet this requirement, we developed a fast detection with virtual router redundancy protocol (FDVRRP) in which VRRP routers are notified promptly about a network failure by the bidirectional forwarding detection (BFD) protocol [18,19]. Accordingly, they can then directly act as the master routers.

For the implementation of FDVRRP, we utilized an open-source–based network operation system, referred to as an open neutralized network operating system (OpenN2OS). It is a network software framework installed on networking equipment that supports various network functions. Our FDVRRP was implemented into OpenN2OS and was loaded as a module. In the performance test of the FDVRRP, we installed OpenN2OS on an ×86 software router using a virtual machine and analyzed its failover performance. Based on the failover test, we verified that the packet loss was reduced significantly during a failover of the FDVRRP in comparison to VRRP.

The remainder of this study is organized as follows: in Section 2, we provide some background to the present topic, and describe the OpenN2OS system architecture, VRRP, and the BFD protocol. In Section 3, we provide the details and operation mechanism of FDVRRP. In Section 4, we introduce the methodology of the performance test. In Section 5, we analyze the performance test and its results. Finally, the concluding remarks are outlined in Section 6.

2 | BACKGROUND

2.1 | OpenN2OS

OpenN2OS [20] is a network operation system, such as Quagga, ZebOS, and Cisco IOS, which is installed on networking equipment. However, contrary to the proprietary NOS, the OpenN2OS is an open architecture software framework that can adopt various networking techniques. It also orients an open platform that supports all types of networking devices. OpenN2OS features a network service with high availability, high modularity, and a hardware-independent hardware abstraction layer (HAL) framework.

Figure 2 shows the overall framework of OpenN2OS. Currently, OpenN2OS supports various networking protocols, such as L2/L3 (eg, STP, MSTP, RSTP, LACP, LLDP, RIP, OSPF, ISIS, VRRP, and BFD), BGP, and MPLS. During the operation of OpenN2OS, administrators or operators can configure network protocols and network interfaces based on the command line interface (CLI). The OpenN2OS source code and development documents can be downloaded at https://openn2os.etri.re.kr.

2.2 | VRRP

VRRP is an open standard. It was designed by IETF in 1999 to handle a single point of failure. VRRP specifies an election protocol that dynamically assigns the responsibility of a virtual router to one of the VRRP routers in a LAN. The VRRP router elected as the master controls the IP address(es) associated with the virtual router, and forwards packets sent to these IP addresses. The master router sends an advertisement packet to the backup routers at successive advertisement intervals (set to 1 s by default). If an advertisement packet is not received by the backup routers within a period of a few seconds (3× advertisement interval + skew time), the backup router that has the highest priority becomes the master router. The skew time is a variation used to skew a timer, which is calculated according to the formula ((256-priority)/256) s.

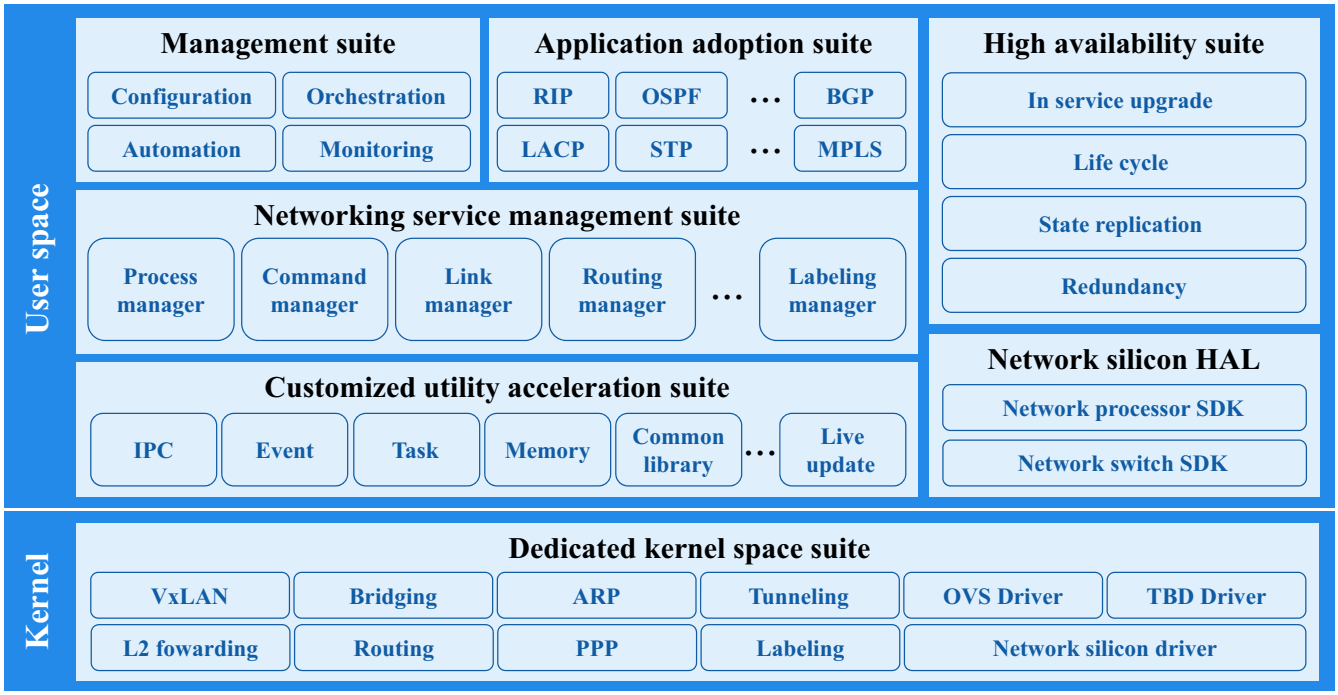


FIGURE 2 OpenN2OS framework

The advantage gained from using VRRP is high availability in the case of a network failure without the need to configure dynamic routing or router discovery protocols at every end-host.

2.3 | BFD protocol

The BFD protocol is designed to provide a low-overhead, and a fast detection of link failures on any type of path, including direct physical links, virtual circuits, tunnels, MPLS label switched paths (LSPs), and multihop routed paths. Furthermore, it operates independently on the transmission media, data protocol, and routing protocol, without any need to modify the existing protocols. BFD nodes send BFD packets periodically over each path between any two nodes. If a node does not receive BFD packets for a certain period of time, some components in that particular bidirectional path are assumed to have failed. In certain instances, BFD nodes may not send periodic BFD packets to reduce the packet overhead.

3 | OPERATION MECHANISM OF FDVRRP

In this section, we describe the FDVRRP operation mechanism on the OpenN2OS framework. When a VRRP group is created on a VRRP router, the router acts as a master or backup router through a master election procedure. After the election, the master router sends a VRRP advertisement packet every second, whereas the backup routers verify the reception of the VRRP advertisement packet. If the received packet is normal and the priority is higher than its own priority, the backup router resets the *master down timer*, which is a regular timer calculated as (3 × advertisement interval + skew time). If the master down timer has expired the backup router becomes the master router, and it starts to send the VRRP advertisement packet. In general, the expiration of the master down timer is caused by the fact that the backup router cannot receive any packets. In other words, this may occur when the master router has failed, or the link between the VRRP routers is down. In any case, it takes more than 3 s for VRRP routers to conduct a complete failover. However, this period is too long to provide a highly available network service.

To reduce the failover time, backup routers need to be aware of a network failure before the master down timer expires. To do so, a VRRP engine interworks with a BFD engine that continually senses the link state between the VRRP routers. As shown in Figure 3, the interaction procedure is as follows: (a) a VRRP engine registers session information of interest with the local IP address and peer IP address into a BFD engine; (b) after the registration, the BFD engine continues to detect the session status and notifies the VRRP engine when the BFD session status is changed (namely, up →down or down →up); and (c) when the VRRP engine receives an event message on a BFD session which is down, it promptly starts changing from a backup to a master router. The interaction between the VRRP and BFD engines is based on the IPC/Event manager, which is one of the basic operations in OpenN2OS (Figure 3).

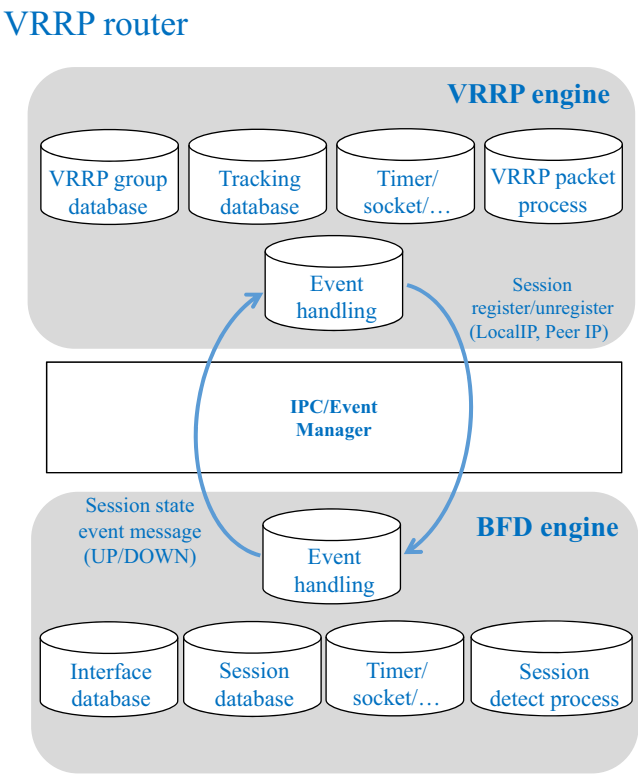


FIGURE 3 Operation mechanism of FDVRRP

4 | METHODOLOGY

To execute the performance test of FDVRRP, we set up a test environment using virtual machines (Ubuntu 14.04) consisting of one server, two routers, one switch, and two end-hosts, as shown in Figure 4. Router-1 and Router-2 are VRRP routers, and Switch-1 is used as an L2 switch for traffic forwarding. We installed OpenN2OS on Router-1, Router-2, and then enabled the VRRP and BFD protocols on these routers.

For a VRRP operation, we should first set up a virtual IP address with a VRRP group number. All routers in the same VRRP group must be configured with the same IP address. Otherwise, they cannot communicate with each other. We configured the VRRP routers with the VRRP group number 1 and the virtual IP address of 199.0.1.1. Using this test environment, we analyzed the fail-over performance of two different configurations, that is, the (1) VRRP and (2) FDVRRP configurations.

4.1 | VRRP configuration

We set up the VRRP configuration at the interface eth1 of Router-1 and Router-2 according to the following commands:

Router-1(config)#
Router-1(config)#interface eth1
Router-1(interface)#vrrp 1 ip 199.0.1.1
Router-1(interface)#vrrp 1 priority 200

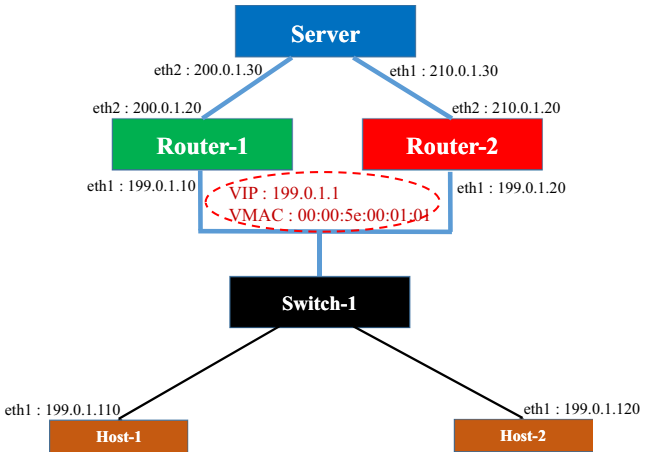


FIGURE 4 VRRP test topology

Router-2(config)#
Router-2(config)#interface eth1
Router-2(interface)#vrrp 1 ip 199.0.1.1
Router-2(interface)#vrrp 1 priority 100

Because the priority of Router-1 (200) is higher than that of Router-2 (100) in accordance with the master election procedure, Router-1 serves as the master router at the beginning. Subsequently, Router-1 adds the virtual IP address (199.0.1.1) as the secondary IP address on the interface eth1, and forwards packets sent to this IP address. Figure 5 shows the VRRP status information of each router.

4.2 | FDVRRP configuration

To make the VRRP engine interact with the BFD engine, we should add a BFD configuration on the interface eth1 of each router. The BFD configuration commands are as follows,

Router-1(config)#
Router-1(config)#interface eth1
Router-1(interface)#bfd interval 300 min-rx 150 multiplier 3
Router-1(interface)#vrrp 1 bfd 199.0.1.20 199.0.1.10
Router-2(config)#
Router-2(config)#interface eth1
Router-2(interface)#bfd interval 300 min-rx 150 multiplier 3
Router-2(interface)#vrrp 1 bfd 199.0.1.10 199.0.1.20

First, we set up the BFD protocol variables: *interval* denotes the desired min transmission interval value (ms), and *min-rx* denotes the required min reception interval value (ms) for a BFD packet. According to this command, the BFD protocol initiates a BFD operation at the interface. Subsequently, we register the BFD session of interest using the information on the peer IP and local IP addresses, as mentioned in Section 3. For example, in the case of Router-1, the peer IP address is 199.0.1.20 and the local IP address is 199.0.1.10. After the registration, the BFD protocol periodically detects a link failure at the BFD

```
Router-1(exec)#
Router-1(exec)#show ip vrrp status
VRRP VERSION 2
eth1 - vrrp group 1
        State is MASTER
        Virtual ip address is 199.0.1.1
        Virtual mac address is 00:00:5e:00:01:01
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 200
        No authentication
        No object tracking
Router-1(exec)#
```

(A)

```
Router-2(exec)#
Router-2(exec)#show ip vrrp status
VRRP VERSION 2
eth1 - vrrp group 1
        State is BACKUP
        Virtual ip address is 199.0.1.1
        Virtual mac address is 00:00:5e:00:01:01
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 100
        No authentication
        No object tracking
Router-2(exec)#
```

(B)

FIGURE 5 VRRP status information: (A) Router-1 serves as the master router and (B) Router-2 serves as the backup router

session by sending and receiving BFD packets. If a failure is detected, the VRRP engine is notified immediately, and the router then promptly changes its status from backup to master. Figure 6 shows the FDVRRP status information of Router-1 and Router-2.

5 | PERFORMANCE TEST AND RESULTS

In this section, we describe the following tests conducted to measure the failover performance, restoration performance, effect of the VRRP advertisement interval, effect of the packet input rate, BFD packet overhead, and load-balancing performance between the VRRP routers. The major benefits of FDVRRP are the very fast failure detection and the failover with a low-packet overhead. Consideration of the failover performance outcome indicates that FDVRRP is almost two times faster than VRRP. Furthermore, FDVRRP significantly reduces the packet loss during the failover, regardless of the VRRP advertisement interval or the packet input rate.

5.1 | Test scenario

To generate traffic from Host-1 and Host-2 to the server, as shown in Figure 4, we used the well-known bandwidth measurement tool, *iperf*. This tool helped us measure the active bandwidth between the client and the server. In this scenario, Host-1 and Host-2 become *iperf clients*, whereas the server acts as an *iperf server*. Upon running *iperf*, each host simultaneously sends UDP packets to the server at 10 Mbps. In all the tests, the UDP packet size is constant and equal to 32 bytes. Accordingly, all the traffic from the hosts will arrive at the server that passes through the master router.

5.2 | Failover performance

First, we conducted a failover test when the master router was disconnected. Based on the configuration mentioned in Section 4, the current master router is Router-1. Figure 7 shows the traffic bandwidth passing through the interface eth2 of Router-1 and Router-2. Before the disconnection, all packets from the hosts pass through Router-1, and the total bandwidth is approximately 20 Mbps (10 Mbps from each host). Subsequently, we shut down the interface eth1 of Router-1. As a result, all packets were instantly blocked until Router-2 acted as the master router for routing all the packets. In this study, we called the duration during which the packet was blocked as the *failover time*. In the VRRP configuration case, the failover time lasted approximately 4 s, as shown in Figure 7A. Meanwhile, we can reduce the failover time by

```
Router-1(exec)#
Router-1(exec)#show ip vrrp status
VRRP VERSION 2
eth1 - vrrp group 1
        State is MASTER
        Virtual ip address is 199.0.1.1
        Virtual mac address is 00:00:5e:00:01:01
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 200
        No authentication
        bfd enabled : peerAddr(199.0.1.20) localAddr(199.0.1.10)
        No object tracking
Router-1(exec)#
```

(A)

```
Router-2(exec)#
Router-2(exec)#show ip vrrp status
VRRP VERSION 2
eth1 - vrrp group 1
        State is BACKUP
        Virtual ip address is 199.0.1.1
        Virtual mac address is 00:00:5e:00:01:01
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 100
        No authentication
        bfd enabled : peerAddr(199.0.1.10) localAddr(199.0.1.20)
        No object tracking
Router-2(exec)#
```

(B)

FIGURE 6 FDVRRP status information: (A) Router-1 is the master. The peer IP address is 199.01.20 and the local IP address is 199.0.1.10 and (B) Router-2 is backup. Peer IP address is 199.01.10 and local IP address is 199.0.1.20

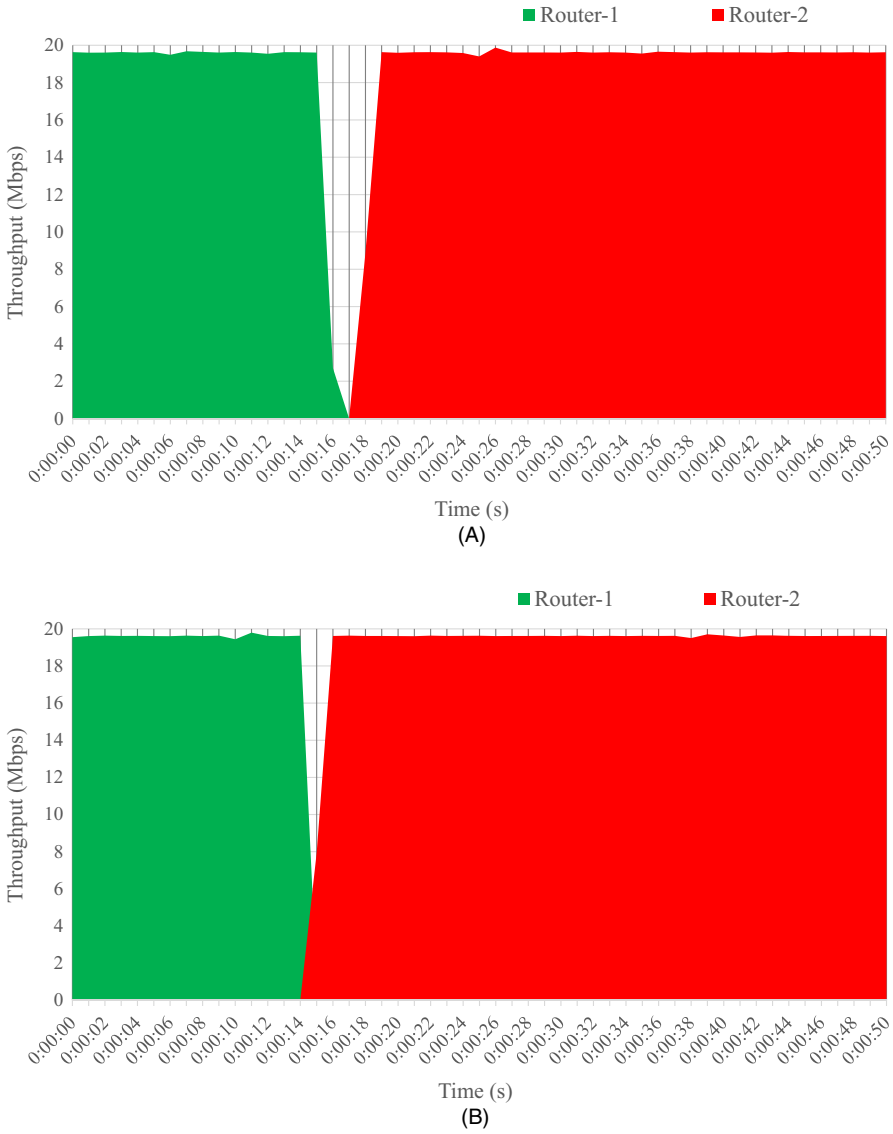


FIGURE 7 Failover performance of VRRP and FDVRRP. (A) VRRP: The failover time is approximately 4 s. (B) FDVRRP: The failover time is approximately 2 s

half (2 s) by virtue of FDVRRP, as shown in Figure 7B. The improvement of the performance of FDVRRP was attributed to a specific mechanism. Whenever the VRRP engine was notified by the BFD engine that a BFD session was down, it instantly switched to the master router regardless of the master down timer.

5.3 | Restoration performance

We conducted a restoration test (as an additional performance test) when the previous master router (Router-1 in this example) was reconnected. In this way, we could control the preemption mode of the VRRP routers. By default, the preemption mode was enabled so that when a higher priority backup router became available, it was elected as the master router again. However, if the preemption mode was disabled, the backup router that had been elected to become the master router remained in the master state, even if the original master router recovered. In the case of the restoration test, we considered that the preemption mode was enabled by default. Initially, all the packets from the hosts passed through Router-2 because Router-1 was disconnected. We then reconnected the interface eth1 of Router-1 so that it can serve as the master router again. In this study, we defined the "restoration time" as the time required by Router-1 to become the master router again in the case of a link restoration. As shown in Figure 8, the restoration time takes approximately 2 s for both the VRRP and FDVRRP configurations. This result was reasonable for both configurations because Switch-1 needed time to update its L2 table through MAC learning to forward packets to the restored path.

5.4 | Effect of VRRP advertisement interval

We also analyzed the effect of the VRRP advertisement interval on the packet loss during the failover time. We established a failover scenario as indicated in Section 4.2, but with a different VRRP advertisement interval. We fixed the

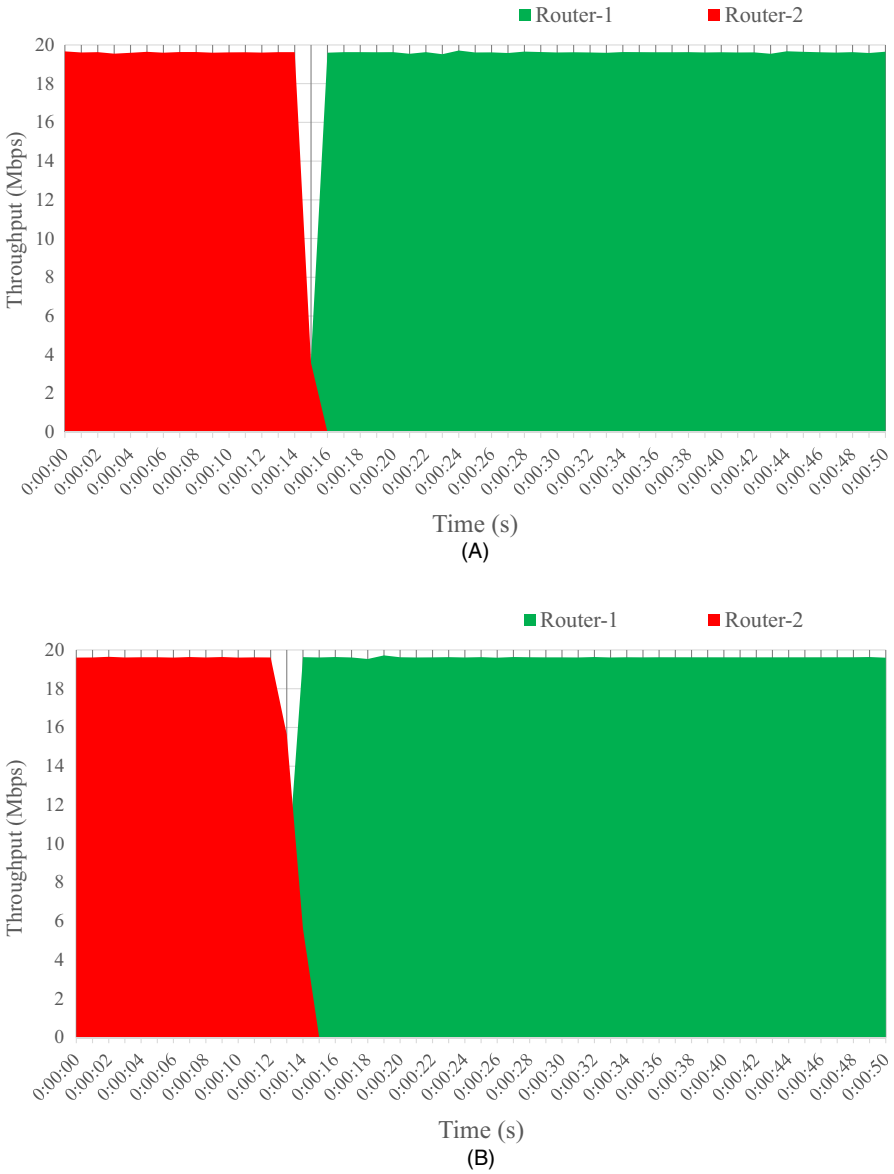


FIGURE 8 Restoration performances of VRRP and FDVRRP. (A) VRRP: The restoration time is approximately 2 s. (B) FDVRRP: The restoration time is approximately 2 s

packet input rate at 50 packets per second and sent packets for 20 s (this was adequate compared to the failover time). Figure 9 shows the number of lost packets during the failover time as a function of the VRRP advertisement interval. When the VRRP advertisement interval is 1 s, approximately 120 packets from a total of 1,000 packets (12%) are lost when the VRRP configuration is used. Conversely, just 26 packets from a total of 1,000 packets (2.6%) are lost when the FDVRRP configuration is used. Furthermore, the packet loss gap became larger as the VRRP advertisement interval increased. Specifically, 300 packets were lost (30%) when the VRRP configuration was used, while 28 packets were lost (2.8%) when the FDVRRP configuration was used and when the VRRP advertisement interval was 3 s (these rates were also estimated based on the same total number of dispatched packets). This performance improvement was derived owing the merits of FDVRRP given that link failures

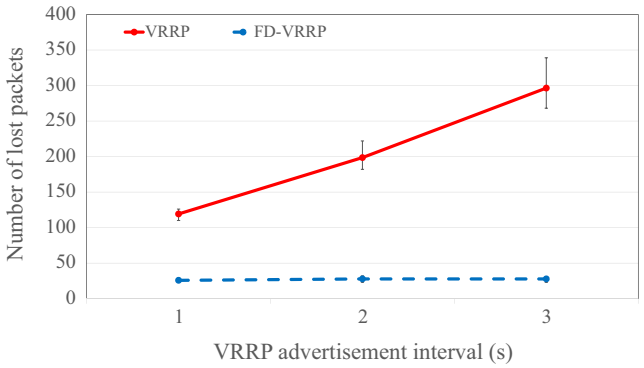


FIGURE 9 Effects of VRRP advertisement interval on the packet loss during a failover

were quickly detected and the backup router instantly acted as the master router, regardless of the VRRP advertisement interval.

5.5 | Effects of packet input rate

The packet input rate also has an influence on the packet loss during the failover time. In this test, we set the VRRP advertisement interval at 1 s while we increased the packet input rate from 1 packet per second to 100 packets per second. For each input rate, the number of test packets was 1,000. As shown in Figure 10, both VRRP and FDVRRP exhibit increased packet loss rates as the packet input rate increases. The gap in the packet loss performance may not be too large when the packet input rate is very low (approximately 1 packet per second, which is a rare case). However, the performance gap increased as the packet input rate increased. When the packet input rate was 5 packets per second, 16 packets (1.6%) were lost when the VRRP configuration was used, but only four packets (0.4%) were lost when the FDVRRP configuration was used. Furthermore, when the packet input rate was 100 packets per second, 224 packets (22.4%) were lost when the VRRP configuration was used, but only 66 packets (6.6%) were lost when the FDVRRP configuration was used. We verified that our FDVRRP reduced the number of lost packets by almost 75% compared with VRRP, and this effectiveness will be stronger when the incoming traffic rate is significantly large, such as in real-time video gaming and virtual/augmented reality applications.

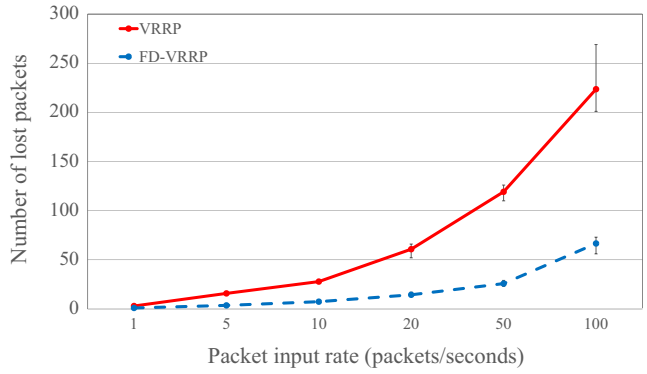


FIGURE 10 Effects of the packet input rate on the packet loss during a failover

5.6 | BFD packet overhead

To measure the BFD packet overhead in a FDVRRP system, we captured the BFD packets to calculate its transmission rate. Figure 11 shows the BFD packet rate at the interface eth1 of Router-1. The input rate indicates the received BFD packet rate, and the output rate indicates the transmitted BFD packet rate. We verified that the input rate was under 2 Kbps, and the output rate was under 2.5 Kbps. Considering the fact that current routers achieve the maximum throughput of over 100 Mbps, this BFD packet overhead is considered as negligible.

5.7 | Load balancing between VRRP routers

To achieve load balancing between the VRRP routers, the routers operated with multiple VRRP groups. For example, Router-1 acted as the master router for the VRRP group 1, and as the backup router for the VRRP group 2, whereas Router-2 acted as the master router for the VRRP group 2, and as the backup router for the VRRP group 1. To accomplish this, each VRRP group must have different virtual IP addresses. In this test, the virtual IP address for the VRRP group 2 was set to 199.0.1.2. The multiple VRRP group scenario was configured based on the use of the following commands:

Router-1(config)#
Router-1(config)#interface eth1
Router-1(interface)#vrrp 1 ip 199.0.1.1
Router-1(interface)#vrrp 1 priority 200
Router-1(interface)#vrrp 2 ip 199.0.1.2
Router-1(interface)#vrrp 2 priority 100
Router-2(config)#
Router-2(config)#interface eth1
Router-2(interface)#vrrp 1 ip 199.0.1.1
Router-2(interface)#vrrp 1 priority 100
Router-2(interface)#vrrp 2 ip 199.0.1.2
Router-2(interface)#vrrp 2 priority 200

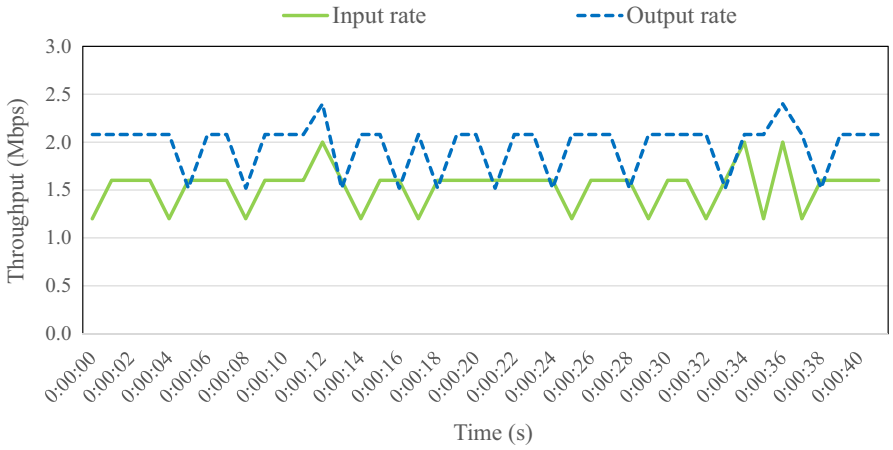
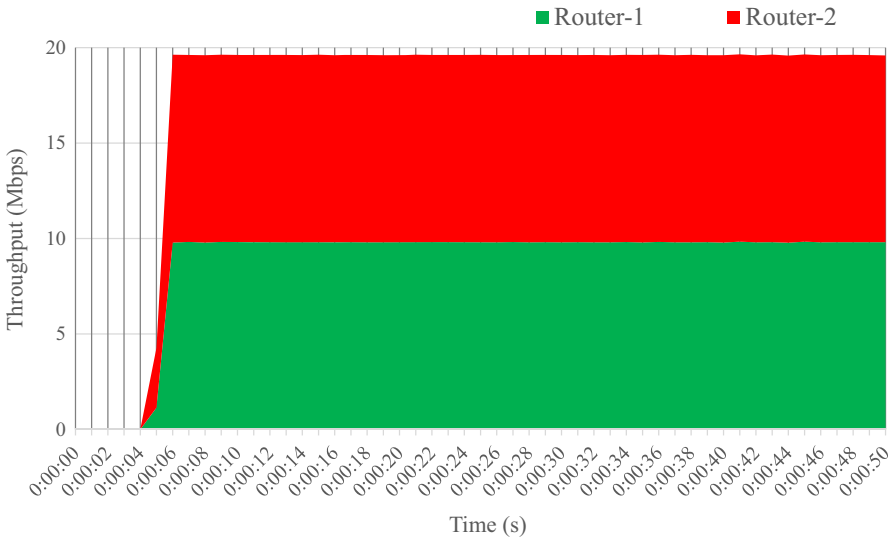


FIGURE 11 BFD packet overhead




```
Router-1(exec)#show ip vrrp status
VRRP VERSION 2
eth1 - vrrp group 1
        State is MASTER
        Virtual ip address is 199.0.1.1
        Virtual mac address is 00:00:5e:00:01:01
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 200
        No authentication
        bfd enabled : peerAddr(199.0.1.20) localAddr(199.0.1.10)
        No object tracking
eth1 - vrrp group 2
        State is BACKUP
        Virtual ip address is 199.0.1.2
        Virtual mac address is 00:00:5e:00:01:02
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 100
        No authentication
        bfd enabled : peerAddr(199.0.1.20) localAddr(199.0.1.10)
        No object tracking
```

(A)

```
Router-2(exec)#show ip vrrp status
VRRP VERSION 2
eth1 - vrrp group 1
        State is BACKUP
        Virtual ip address is 199.0.1.1
        Virtual mac address is 00:00:5e:00:01:01
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 100
        No authentication
        bfd enabled : peerAddr(199.0.1.10) localAddr(199.0.1.20)
        No object tracking
eth1 - vrrp group 2
        State is MASTER
        Virtual ip address is 199.0.1.2
        Virtual mac address is 00:00:5e:00:01:02
        Advertisement interval is 1 sec
        Preemption is enabled
        Priority is 200
        No authentication
        bfd enabled : peerAddr(199.0.1.10) localAddr(199.0.1.20)
        No object tracking
```

(B)

FIGURE 12 Load-balancing between VRRP routers (10 Mbps per router)

FIGURE 13 FDVRRP configurations with multiple VRRP groups: (A) Router-1 is the master router for VRRP group 1 and (B) Router-2 is the master router for VRRP group 2

After the configuration of the VRRP routers, we set up the default gateway IP addresses of Host-1 and Host-2 to 199.0.1.1 and 199.0.1.2, respectively. Each host simultaneously sent UDP packets to the server at 10 Mbps. Figure 12 clearly shows that the traffic is evenly distributed to each router. This is because the traffic from Host-1 passes through the master router of the VRRP group 1 (Router-1), whereas the traffic from Host-2 passes through the master router of VRRP group 2 (Router-2). Figure 13 shows the FDVRRP configuration with multiple VRRP groups. Router-1 is the master router for the VRRP group 1, whereas Router-2 is the master router for the VRRP group 2.

6 | CONCLUSIONS

Within a LAN, VRRP has been suggested as a method to achieve a highly available and reliable network service, even during network failures. However, when there is an increasing demand for real-time services and an increase in the number of applications that are sensitive to packet loss, the traditional VRRP reaches its support limit because it cannot cope promptly with network failures that occur in the path between the VRRP routers. To address these weak points, we proposed the use of FDVRRP in which the backup router quickly detected link failures and immediately became the master router. Based on a failover performance test, we verified that FDVRRP exhibited increased capacity for very fast failure detections and failovers with low-packet overhead. Its response was almost improved by a factor of two compared to VRRP. Furthermore, FDVRRP greatly reduced packet loss during the failover time, regardless of the VRRP advertisement interval or the packet input rate. In future work, we will consider the interworking of the BFD protocol with other L3 protocols, such as OSPF, ISIS, and BGP, to improve the L3 routing in the case of link failures.

ACKNOWLEDGMENTS

This work was supported by the ICT R&D program of MSIT/IITP [R0101-16-0070, Development of the High Availability Network Operating System for supporting Non-Stop Active Routing], Republic of Korea.

ORCID

Changsik Lee https://orcid.org/0000-0002-3825-7317

REFERENCES

1. N. Kimura and S. Latifi. *A survey on data compression in wireless sensor networks*, Proc. Int. Conf. Inf. Technol.: Coding Comput., Las Vegas, NV, USA, 2005, pp. 8–13.
2. H. Hadizadeh and I. V.Bajic, *Saliency-aware video compression*, IEEE Trans. Image Process. **23** (2014), 19–33.
3. T. Maples and G. Spanos. *Performance study of a selective encryption scheme for the security of networked, real-time video*, Int. Conf. Comput. Commun. Netw., Las Vegas, NV, USA, 1995, pp. 2–10.
4. C.-P. Wu and C.-C. J. Kuo, *Design of integrated multimedia compression and encryption systems*, IEEE Trans. Multimedia **7** (2005), 828–839.
5. D. Wu, Y. T. Hou, and Y.-Q. Zhang, *Transporting real-time video over the internet: challenges and approaches*, Proc. IEEE **88** (2000), 1855–1875.
6. J. Apostolopoulos, *Reliable video communication over lossy packet networks using multiple state encoding and path diversity*, Proc. SPIE Visual Commun. Image Process. **430** (2001), 392–409.
7. G. Singh and M. V. Raju, *Dual gateway routing protocol*, Int. Conf. Comput. Sci., Phagwara, India, 2012, pp. 350–355.
8. T. Chia-Tai, J. Rong-Hong, and W. Kuochen, *Optimal redundancy allocation for high availability routers*, Int. J. Commun. Syst. **23** (2010), 1581–1599.
9. T. Li et al., *RFC 2281, Cisco hot standby router protocol (HSRP)*, Internet Engineering Task Force, 1998, available at http://www.ietf.org/rfc/rfc2281.txt.
10. IETF, 2002. [Online]. available at https://tools.ietf.org/html/draft-ietf-vrrp-spec-v2-06
11. IETF, 1998, [Online]. available at https://tools.ietf.org/html/rfc2338
12. IETF, 2004, [Online]. available at https://tools.ietf.org/html/rfc3768
13. J. Etienne, *VRRPd: Overview, implementation, and usage*, Ottawa Linux Symp, Ottawa, Canada, 2001.
14. J. Ranta, *Router redundancy and scalability using clustering, Seminar on Internet Working*, (A. Ylä-Jääski, and N. Kasinskaja, eds.), 2014, available at http://www.tml.hut.fi/Studies/T-110.551/2004/papers/Ranta.pdf.
15. O. V. Lemeshko et al., *Fault tolerance improvement for core and edge of IP network*, Proc. Int. Sci. Tech. Conf. Comput. Sci. Inf. Technol., Amman, Jordan, 2016, pp. 161–164.
16. O. Lemeshko, O. Yeremenko, and N. Tariki, *Solution for the default gateway protection within fault-tolerant routing in an IP network*, Int. J. Electr. Comput. Eng. Syst. **8** (2017), 19–26.
17. L. et al, *Fault tolerant mechanisms for SDN controllers*, Proc. IEEE Conf. Netw. Funct. Virtualization Softw. Defined Netw., Palo Alto, CA, USA, 2016, pp. 173–178.
18. D. Katz and D. Ward, *Bidirectional forwarding detection (BFD)*, Internet Engineering Task Force, RFC 5880 (Proposed Standard), 2010, available at http://www.ietf.org/rfc/rfc5880.txt.
19. F. Minglei, Z. Le, and Z. Zhu, *BFD-based failure detection and localization in IP over OBS/WDM multilayer network*, Int. J. Commun. Syst. **25** (2012), 277–293.
20. Electronics and Telecommunications Research Institute (ETRI), *Neutralized network operating system*, available at https://openn2os.etri.re.kr.

AUTHOR BIOGRAPHIES

Changsik Lee received his BS degree in electrical engineering from Korea University, Seoul, Rep. of Korea, in 2012, and his MS degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Rep. of Korea, in 2014. Since 2014, he has been with the Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea, where he is currently a researcher. His interests include virtual router redundancy, openflow, edge computing, and machine learning algorithms.

Suncheul Kim received his BS and MS degrees in statistics and computer science from Chungbuk National University, Cheongju, Rep. of Korea, in 1995 and 2000, respectively. Since June 2000, he has been with the Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea, where he is currently a principal researcher. He has primarily focused on the development of routing, multicast, and MPLS protocols for network operating system.

Hoyong Ryu received the BS, MS, and PhD degrees in electronic communication engineering from the Kwangwoon University, Seoul, Rep. of Korea, in 1993, 1995, and 1999, respectively. Since December 1998, he has been with the Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea, where he is a principal member of the engineering staff. His research interests include SDN/NFV platform and edge computing technologies.