Dual-Stack Network Management Through One-Time Authentication Mechanism

YI-CHIH KAO\textsuperscript{1}, JUI-CHUN LIU\textsuperscript{1}, YI-QUAN KE\textsuperscript{1}, SHI-CHUN TSAI\textsuperscript{2}, (Senior Member, IEEE), AND YI-BING LIN\textsuperscript{2}, (Fellow, IEEE)

\textsuperscript{1}Information Technology Service Center, National Chiao Tung University, Hsinchu 30010, Taiwan
\textsuperscript{2}Department of Computer Science, National Chiao Tung University, Hsinchu 30010, Taiwan

Corresponding author: Yi-Chih Kao (ykao@mail.nctu.edu.tw)

This work was financially supported by the Center for Open Intelligent Connectivity from the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

ABSTRACT The exhaustion of IPv4 addresses has led to the rapid implementation of IPv6. However, the design of IPv6 is incompatible with that of its predecessor IPv4 and slows down the development of the IPv4-to-IPv6 migration. Several transitioning mechanisms have been proposed to attain the compatibility of IPv4 and IPv6 to bridge the gap between these two heterogeneous protocols. The two protocols would need to coexist continually before IPv6 completely takes over IPv4. However, the existing captive portal authentication systems generally do not support IPv4/IPv6 dual-stack authentication and lack one-time dual-stack authentication solutions. Upgrading the authentication system has become an urgent problem to be addressed. This study presents dual-stack network management strategies using a novel one-time authentication mechanism for large and complex dual-stack network environments. The proposed authentication system resolves the inconvenience of separate IPv4 and IPv6 authentication and effectively improves the compatibility of the two protocols. Furthermore, authenticating both IPv4 and IPv6 increases the traceability of traffic logs when security attacks occur. The proposed solution is deployed in a campus dormitory environment, and the feasibility and stability are successfully verified.

INDEX TERMS Authentication, dual-stack, IPv6, management.

I. INTRODUCTION

A. THE EMERGENCE OF IPV6

The exhaustion of IPv4 addresses has become a reality. To maintain network services, the introduction of IPv6 addresses is an inevitable step. As the successor of IPv4, IPv6 increases the address length of IPv4 by four times, expanding it from the current 32 bits (4 bytes) to 128 bits (16bytes). As a result, IPv6 offers $3.4 \times 10^{38}$ address spaces, which is a significant increase from the $4.29 \times 10^9$ address space of IPv4, providing a massive number of IP addresses for exploitation. Besides, IPv6 offers notable improvements in terms of Internet Protocol Security (IPSec) and Quality of Service (QoS). The built-in IPSec in IPv6 provides two security mechanisms for data transmission: authentication and encryption. By adding a mandatory Authentication Header, the integrity and non-repudiation of the packet transmission are ensured by the Encapsulating Security Payload on packets encryption to enhance confidentiality and keep transmitted contents from eavesdropping. Another essential feature of IPSec is the provision of Virtual Private Network (VPN) functionality, enabling a more secure and reliable VPN in IPv6. At the same time, QoS uses the Flow Label field of the IPv6 header to meet the low latency requirements of multimedia applications (e.g., VoIP and video) and provide highly efficient network transmission quality.

IPv6 is widely used nowadays, according to the statistics report from Google [2], the global IPv6 deployment and adoption rate reached 25% in 2018. According to the data from Taiwan Network Information Center [3], the IPv6 deployment and adoption rate of Taiwan has increased from 0.38% (67th place in the global ranking) in November 2017 to 34.93% (7th place in the global ranking) in January 2019.

B. IPV4/IPV6 DUAL-STACK

Currently, the majority of network hardware and software systems are operating under IPv4. Once the network
environment is upgraded to IPv6, the end-to-end related connections, routers, switches, firewalls, intrusion detection systems, and web applications must support IPv6 to maintain normal network functions. However, the complexity and uncertainty of these network components often make users hesitate.

IPv6 is expected to replace the role of IPv4 on the Internet completely. Until then, these two heterogeneous protocols still need to coexist for a long time. Given the differences in the design of these protocols, numerous IPv4/IPv6 transitioning mechanisms have been developed. The most common techniques include dual-stack, tunneling, and translation. Since tunneling and translation have performance bottlenecks [4], they are only short-term solutions. Only the dual-stack approach can gradually evolve from IPv4 dominant network to IPv4/IPv6 dual-stack network, finally reaching an entirely IPv6-based network. Therefore, this study mainly focuses on the dual-stack technique.

With the continuous development of IPv6, effectively authenticating the identity of users has become a research subject. Nevertheless, the majority of current captive portals are designed based on IPv4 and cannot fully support IPv6 [13]. Therefore, when a device accesses the network with IPv4 and IPv6 addresses, the IPv4 address needs to pass authentication, whereas the IPv6 address can access the network without any authentication [12]. Since the majority of authentication systems lack effective control mechanisms over the IPv4/IPv6 dual-stack access, they can only authenticate one type of protocol at a time, either IPv4 or IPv6. Such authentication systems carry out authentication twice at the user’s IPv4 and IPv6, respectively [11], [13]. That is, after IPv4 has been authenticated, the user has to be authenticated again if he/she needs to access IPv6 applications. Similarly, for IPv6, the user has to be authenticated again once if he/she needs to access IPv4 applications. Such inconvenience may deter users from migrating to IPv6. Even worse, the incapability of some authentication systems to authenticate IPv6 addresses can result in security concerns, necessitating an effective dual-stack authentication mechanism to overcome these problems.

C. DUAL-STACK NETWORK MANAGEMENT

In large and complex network environments such as a campus dormitory, effectively managing IPv4 and IPv6 network services could be a nightmare for network administrators. Therefore, this paper proposes a series of dual-stack network management strategies to ensure controllability over a large number of users. First, we discuss the existing techniques for IPv4 and IPv6 address allocation. Then, we propose a novel dual-stack authentication mechanism for environments where IPv4 and IPv6 coexist. This mechanism enables efficient and convenient one-time authentication. The capability of tracking and monitoring the IPv4 and IPv6 of authenticated users is achieved by combining the strategies mentioned above, which helps mitigating security attacks. Note that an improperly implemented dual-stack authentication may sacrifice the manageability and security of IPv4 and IPv6 traffic.

The rest of this paper is organized as follows. Section II overviews the techniques and literature related to IPv4 and IPv6 address allocation, as well as authentication in dual-stack network environments. Section III describes the current authentication system architecture deployed across a campus dormitory and outlines a novel one-time authentication mechanism for our dual-stack network environment. Section IV presents the experiments conducted to verify the functionality and stability of the proposed one-time authentication architecture. Finally, Section V provides conclusions and suggestions for future work.

II. BACKGROUND AND RELATED WORK

This section overviews the existing techniques related to address allocation in dual-stack networks, namely, DHCP Option 82 and IPv6 Address Auto-Configuration. Also, the IPv4 and IPv6 transitioning mechanisms are briefly introduced. Finally, previous studies on Media Access Control (MAC) based authentication and dual-stack authentication mechanisms are surveyed.

A. DHCP OPTION 82

As defined in RFC3046 [5], DHCP Option 82 is the Relay Agent Information Option in the DHCP packet. When Option 82 is enabled in the network, a network device (DHCP client) can send a DHCP request to the DHCP server. In this case, the switch (DHCP relay agent) injects additional information called Relay Agent Information specifying the details about the switch and port to which the client is connected. When the DHCP server receives the packet, it parses the Option 82 information to identify which IPv4 address to be assigned to this client. Hence, DHCP servers can be configured to always assign the same IPv4 address to the devices on a specific port. Note this way is more convenient for the network administrator to manage specific areas by providing particular sets of dynamic IPs from the DHCP pool and minimize IP conflict or collision occurrences.

B. IPV6 ADDRESS AUTO-CONFIGURATION

There are two types of IPv6 network address configuration approaches: static and dynamic. Stateful and Stateless Address Auto-Configuration [6] are examples of the dynamic address configuration approaches. The Stateful DHCPv6 inherits auto-configuration service from the IPv4 DHCP. Since the IPv6 address is assigned via DHCPv6, the correspondence between IPv6 and MAC addresses is recorded and maintained in a binding table that is updated periodically. Hence, this configuration approach is called Stateful.

The Stateless Address Auto-Configuration (SLAAC) is another auto-configuration approach. The information of the IPv6 prefix and the default gateway is obtained from the router advertisement (RA) packet, and the IEEE defined 64-bit extended unique identifier (EUI-64) is used to allow
the host to assign a unique 64-bit IPv6 interface identifier to itself. EUI-64 automatically configures the IPv6 address of the host based on the MAC address of the original interface plus a fixed prefix. In other words, a complete IPv6 address in SLAAC is formed by the RA-assigned prefix and the automatically generated interface ID by EUI-64. This plug-and-play feature helps simplify the host configuration and reduce the burden of end-users.

C. IPV4 AND IPV6 TRANSITIONING MECHANISM

The commonly used IPv4 and IPv6 transitioning mechanisms include dual-stack, tunneling, and translation. Dual-stack is the most popular and widely used one that turns an IPv4-capable device into supporting IPv4 and IPv6 simultaneously. A dual-stack-capable device not only enables IPv4 and IPv6 to coexist but also ensures their interoperability and backward compatibility. Tunneling encapsulates an IPv4 header outside the IPv6 packet, allowing IPv6-capable network devices at both ends to communicate via the IPv4 tunnel and providing IPv6 virtual connections over the IPv4 physical network. IPv4/IPv6 translation is similar to the network address translation, which utilizes a router or a default gateway at the IPv4 or IPv6 border to convert the IPv4 header to the IPv6 header or vice versa, allowing IPv4 and IPv6 network devices to communicate with each other.

D. MAC AUTHENTICATION

MAC authentication is an approach authenticating a device based on its MAC address that must match a predefined IP address. Kao et al. [7] summarized the specific process of MAC authentication: if a user device fails the authentication, it will be redirected to the captive portal where the user has to enter his/her credentials, which will be stored in the database together with the device’s MAC address. When the user connects to the Internet via the same device next time, the device will automatically pass the identity authentication after verifying its MAC address stored in the database.

The authentication mechanism based on software-defined networking proposed by Lu et al. [8] contains an authentication table module that maintains a sheet for storing the collected users’ device information. The sheet is indexed by the MAC address to avoid duplicate entries. The verification module parses all packet-in ICMPv6 packets to filter out Neighbor Discovery Protocol (NDP) packets to check whether the source MAC and IPv6 addresses match the information stored in the authentication table. Despite exploiting MAC address as the key value, the approach proposed by Lu et al. only offers an authentication mechanism for IPv6 without considering IPv4/IPv6 dual-stack authentication.

E. DUAL-STACK AUTHENTICATION MECHANISM

As mentioned by Huang et al. [9], many users may access multiple network resources during a work session. Thus, user devices have to be authenticated via separate login procedures for each IP address to gain access to one or more network resources. The productivity of users can be decreased significantly due to many separate authentication procedures. Hence, we explore several dual-stack authentication mechanisms to find a better technique that solves this problem.

The framework proposed by Bennett III et al. [10] authenticates user devices through discovering their IP versions to determine whether they are authorized to access data via IPv4, IPv6, or both. If authorization information indicates that the user can only access the data through IPv4 instead of IPv6, the authentication device only triggers the necessary steps to authenticate IPv4. Thus additional resources are not consumed to authenticate the user device’s IPv6 and vice versa. However, this solution has not been tested in a working environment, and there exist performance concerns when applied to complex network environments.

Sanguanpong and Koht-Arsa [11] proposed a mechanism called Dual Address Discovery (DAD) to avoid duplicate authentication under the dual-stack network environment. By embedding two image tags in the login page, where one of the DNS maps to the IPv4 address, and the other maps to the IPv6 address, these two separate protocols are bound together with an identical hash code. Once the user obtains both IPv4 and IPv6 addresses, the authentication server can associate IPv4 and IPv6 with the same hash code, thereby authenticating the two protocols at the same time. Such an approach can effectively save time by preventing repeated authentication. While the architecture of DAD is relatively simple and easy to deploy, there are still some problems to be solved. For example, it requires the users to have both IPv4 and IPv6 addresses during the authentication process to achieve one-time authentication. If users complete the authentication in a pure IPv4 environment and then transfer to a dual-stack environment, the authentication procedure must be repeated to let the authentication server to associate IPv4 and IPv6. Sanguanpong et al. did not elaborate on the system architecture of their tested environment, nor did they verify and evaluate its performance, stability, and feasibility in a working network environment.

According to the method designed by Lin [12], the authentication system controls the address allocation process of the second IP address after the first one is authenticated. Then, the authentication system stores both IPv4 and IPv6 addresses, along with other information in the user information table, and manages dual-stack users’ network access according to the stored control policy. This approach solves the problem that any randomly configured address can access the service through a network device without authentication. For example, when the portal authenticates an IPv4 user, the user information is added to the database, and the RA is sent to the user to notify him/her about the IPv6 address configuration method. Similarly, after the authentication of IPv6, the user information is added to the database, and a DHCPv4 discovery message is sent to the user to notify the user about the IPv4 address configuration method, thereby achieving the access control of the dual-stack user. However,
TABLE 1. Summary of dual-stack authentication mechanisms.

| Author               | Solution                                                                 | Benefit                                                                                     | Drawback                                                                                     |
|----------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Bennett III et al. [10] | Determine the IP version of the user and check whether it is authorized to access data via IPv4, IPv6, or both. | It only triggers necessary steps for authentication without authenticating both IPv4 and IPv6. | No field-trial or test in a working environment. A performance issue exists.                 |
| Sanguanpong et al. [11] | Bind two image tags of IPv4 and IPv6 through an identical hash code for further matching. | Effectively reduces repeated authentication. The structure is relatively simple and easy to deploy. | Requiring IPv4 and IPv6 addresses simultaneously while authenticating to achieve one-time authentication. |
| Lin [12]             | Controls and monitors the process of the second IP address configuration after the first IP address is authenticated. | Avoids any randomly configured IP address to access the service through the network device without authentication. | Not applicable to network environments managed centrally only by the upper layer-3 authentication server. |
| Wang [13]            | Use MAC and DUID to match the user’s IPv4 and IPv6, respectively, then bind the above information. | The IP address binding relies only on browser’s JavaScript code and does not require other plug-ins or software. | Requiring IPv4 and IPv6 addresses simultaneously while authenticating to achieve one-time authentication. |

RA must be placed in the lower layer (Gateway) of the network architecture. A typical network does not have an appropriate environment and resources to implement a large amount of authentication equipment. Therefore, this method is not suitable for centralized network environments managed only by the upper layer-3 authentication server.

Wang [13] obtained the IPv4 and IPv6 association of the user by parsing DHCP packets. In the IPv4 environment, the MAC address in the DHCP packet can be used to associate the IPv4 address of the user. In the IPv6 environment, the DHCP Unique Identifier (DUID) identifies the DHCPv6 device in the DHCPv6 packet, thus binding the user DUID with the IPv6 address. The DNS server redirects all requests of the user to the authenticated portal page to attain one-time IPv4/IPv6 dual-stack authentication when the user obtains the IP address. If an unauthenticated user uses IPv4 to access the portal, he/she will be redirected to the login portal together with an encrypted message. Then, a JavaScript code actively triggers the user to access another login portal with IPv6 carrying the same encrypted message. When the portal obtains the user’s IPv4 and IPv6 addresses simultaneously, the binding of the user’s IP addresses is achieved.

As pointed out in [13], traditional methods for binding user MAC and IP addresses for authentication have several problems in the dual-stack environment. First, when the authentication equipment is deployed between the layer-3 switch and the internal network, the user MAC address may be dropped by the routing equipment in-between, preventing the IPv4/IPv6 association of the same user being created. Second, if the stateful auto-configuration is adopted in the DHCPv6 address configuring process, the message passed through the DHCPv6 relay does not contain the MAC address information, and no IPv4/IPv6 association would be established.

Table 1 summarizes the reviewed dual-stack authentication mechanisms. Even though some of these authentication mechanisms can achieve authentication when IPv4 and IPv6 coexist, they lack flexibility in operation. For example, Lin’s solution relies on RA and requires authentication equipment supporting RA, which is not suitable for a network environment managed centrally only by the upper L3 authentication server. The studies by Sanguanpong et al. and Wang adopt the method of embedding the same hash code, requiring both the IPv4 and IPv6 addresses to be present while conducting user authentication to achieve one-time authentication.

III. PROPOSED FRAMEWORK
This section describes the structure of the authentication system deployed in a campus dormitory. It illustrates the address auto-configuration process applied to this versatile dormitory environment considering the convenience and security of dorm users in terms of network service. Furthermore, this section presents the proposed one-time dual-stack authentication mechanism with its functional modules and demonstrates its ability to trace security attacks within the considered domain.

A. AUTHENTICATION SYSTEM ARCHITECTURE
The architecture of the deployed authentication system is illustrated in Fig. 1. The main components of the authentication system include a Core Router, an Authentication Server (Auth Server), an Internal Router, Layer 3 Switches (L3 Switch), a DHCP Server, Layer 2 Switches (L2 Switch), and End User Devices. The Core Router (Fig. 1(a)) serves as the gateway of the entire architecture for external connections. The Auth Server (Fig. 1(b)) is responsible for determining whether the underlying traffic is from an authenticated user. The Internal Router (Fig. 1(c)) is responsible for the congregation of network cables from the L3 Switches (Fig. 1(d)). The DHCP Server (Fig. 1(e)) is connected to the L3 Switch to provide IP addresses automatically. For the network distributing cables of each dormitory, the L3 Switch acts as a gateway connecting to each room’s network ports via L2 Switch (Fig. 1(f)) to serve the End User Devices.
Y.-C. Kao et al.: Dual-Stack Network Management Through One-Time Authentication Mechanism

FIGURE 1. Proposed authentication system architecture.

(Fig. 1(g)). Instead of connecting all L3 Switches directly to the Auth Server to enable the backbone network, the proposed architecture utilizes a router to accommodate the traffic of each L3 Switch. Thus, the Auth Server only needs to manage upward and downward network interfaces, making the network architecture relatively simple and easy to manage.

B. AUTOMATIC ADDRESS ALLOCATION STRATEGIES

1) MOTIVATION
The network environment of university dormitories is often versatile and sophisticated, designed to accommodate a large number of students. Students come and go every year. Thus, the configuration of the university network is constantly changing. To help network administrators to manage such a complex environment, it requires the implementation of a convenient yet secure address auto-configuration process. In the dormitory, we deploy DHCP Option 82 to provide IPv4 addresses based on switch ports, while SLAAC is for allocating IPv6 addresses.

By exploiting DHCP and SLAAC to allocate IPv4 and IPv6 addresses automatically, the problem of manually setting up the network configuration for thousands of users is avoided, which not only simplifies the host configuration process but also relieves the burden of end-users. Furthermore, with Option 82, every switch port is mapped to a specific IP address. It can enhance the manageability of network services. The use of Option 82 can also protect users against security attacks such as spoofing and forging of IP and MAC addresses, making the network environment more secure.

2) MAC PROXY
The network configuration of a dormitory is often dynamic, which creates the issue that a switch port might already bound to the MAC and IP addresses of a particular device when the lease time has not expired. If another device is connected to a port that has a predefined binding rule, the DHCP relay identifier will not match, preventing the new device from obtaining an IP address from the DHCP server. To overcome this problem, we give a novel approach called MAC Proxy is applied, which makes the MAC address of the switch port act as a proxy client for binding an IP address. It improves interoperability by binding the MAC address of the switch port in Option 82, instead of binding the MAC address of a user device. It allows IP addresses to be immediately released and returned to the address pool when DHCP clients are no longer using the IP addresses. When another DHCP client sends a request, the DHCP server can assign the released IP addresses to other clients. Without MAC Proxy, IP addresses may be occupied for the entire lease time, and other DHCP clients would have to wait until the address lease time expires.

C. DUAL-STACK AUTHENTICATION MECHANISM

The automatic address allocation is extensively used in the considered campus dormitory to provide the flexibility of managing and maintaining network services from a centralized position without the need for manual configuration. When a user tries to initiate an Internet connection after obtaining IPv4 and IPv6 addresses, he/she has to be authenticated before accessing the Internet. In this scenario, the user is redirected to the captive portal responsible for the user access control to verify the user identity.

To authenticate IPv4 and IPv6 addresses effectively and seamlessly, one needs a robust dual-stack authentication mechanism. In the following paragraphs, the workflow of the traditional dual-stack authentication mechanism is first described to understand its flaw and inefficiency. The proposed one-time dual-stack authentication mechanism is explained later to emphasize its advantages.

1) TRADITIONAL DUAL-STACK AUTHENTICATION WORKFLOW

Fig. 2 shows the traditional dual-stack authentication mechanism. In the beginning, a user attempts to initiate the first HTTP connection through IPv4 (Fig. 2(a)), the Auth Server finds that the user’s IPv4 address has not been authenticated according to the packet source IP (Fig. 2(b)). The unauthenticated user is then redirected to the login page (Fig. 2(c)), where he/she is required to enter the account name and password to be authenticated (Fig. 2(d)). After recognizing the user’s IPv4 as authenticated (Fig. 2(e)), the Auth Server grants the user access to the network service via IPv4 (Fig. 2(f)). Upon completing the IPv4 authentication, the user can attempt to initiate the connection via IPv6 (Fig. 2(g)). The unauthenticated user is then redirected to the login page again (Fig. 2(h)), where he/she has to re-enter the account name and password for authentication (Fig. 2(i)). After recognizing the user’s IPv6 as authenticated (Fig. 2(k)),
the Auth Server grants the user access to the network service via IPv6 (Fig. 2(l)). Similarly, if the user first passes IPv6 authentication, he/she still has to be authenticated again when using IPv4.

### 2) DEPLOYING THE ONE-TIME DUAL-STACK AUTHENTICATION MECHANISM IN CAMPUS DORMITORY

In the campus dormitory framework, the L3 Switch is a gateway maintaining IPv4 and MAC addresses mapping in the Address Resolution Protocol (ARP) table, as well as IPv6 and MAC addresses mapping in the NDP table. Hence, the L3 Switch has the user information, including IPv4, IPv6, and MAC addresses. Since the user’s MAC address is unique and fixed, the Auth Server can obtain the user information through the Simple Network Management Protocol (SNMP), making it a MAC-based authentication mechanism.

This study proposes a cross-layer-3 MAC authentication solution suitable for dual-stack environments that allows the Auth Server to query the L3 Switch periodically through the SNMP protocol to obtain the user devices’ IPv4, IPv6, and MAC addresses stored in the ARP and NDP tables. It should be noted that although the MAC address of the user device is replaced by that of the switch port when applying MAC Proxy as mentioned previously, the switch port’s MAC address is only transmitted as a proxy in the DHCP relay. Thus, the MAC address displayed in the ARP table still belongs to the user device.

When the L3 Switch receives the request message, it first enquires about the ARP and NDP tables accordingly and sends back the response to the Auth Server. The Auth Server then compares the obtained content with the user IP and MAC addresses. If the MAC address matches the information stored in the Auth Server, the user is authenticated successfully; if the MAC address does not match, the authentication fails. This approach solves the problem that the upper-layer authentication device of the L3 Switch cannot read the user MAC address, and establishes a flexible and easy-to-deploy dual-stack authentication mechanism.

### 3) ONE-TIME DUAL-STACK AUTHENTICATION WORKFLOW

According to the one-time dual-stack authentication mechanism workflow shown in Fig. 3, the L3 Switch records the underlying user information to the ARP and NDP tables (Fig. 3(a)). The Auth Server can then obtain ARP and NDP tables from the L3 Switch via SNMP (Fig. 3(b)). When a user attempts to initiate the first HTTP connection via IPv4 (Fig. 3(c)), the Auth Server compares the packet source IP with that in the ARP table to obtain the MAC address of the user and finds that the user’s MAC address has not been authenticated (Fig. 3(d)). The unauthenticated user is then redirected to the login page (Fig. 3(e)), where he/she is required to enter the account name and password to be authenticated.

---

**FIGURE 2.** Traditional dual-stack authentication mechanism workflow [1].

- (a) HTTP Request through IPv4
- (c) Redirect to login page
- (d) Login
- (e) IPv4 Authenticated
- (f) Internet service through IPv4
- (g) HTTP Request through IPv6
- (i) Redirect to login page again
- (j) Login
- (k) IPv6 Authenticated
- (l) Internet service through IPv6

**FIGURE 3.** One-time dual-stack authentication mechanism workflow [1].

- (a) IPv4 ARP
- (b) Obtain ARP
- (d) MAC address is not authenticated
- (g) IPv4, MAC Authenticated
- (i) HTTP Request through IPv6
- (j) MAC address is authenticated
- (l) Internet service through IPv6
authenticated (Fig. 3(f)). After the Auth Server recognizes the IPv4 and MAC addresses as authenticated (Fig. 3(g)), the user can use the network service via IPv4 (Fig. 3(h)). When the user attempts to use IPv6 to initiate the connection (Fig. 3(i)), the Auth Server compares the packet source IP with that in the NDP table to obtain the MAC address of the user and find that the user’s MAC address has been authenticated (Fig. 3(j)). Therefore, the IPv6 packet is not blocked, and the user is allowed to use the network service via IPv6 without logging again (Fig. 3(k)). Similarly, if a user first passes IPv6 authentication, the Auth Server can identify whether the IPv4 address has passed the authentication using the recorded MAC address and ARP table. Further authentication for the IPv4 address is not required.

4) SUMMARY
The traditional authentication architecture requires separate authentication for IPv4 and IPv6. Some systems only authenticate either IPv4 or IPv6, making users vulnerable to security attacks. In contrast, the proposed authentication mechanism first uses SNMP to obtain the user identity information from the ARP and NDP tables. It then uses the recorded MAC address to authenticate the identity and completes the authentication for IPv4 and IPv6 at the same time. When the connection is initiated by another protocol again, the second login is not required. Hence, the user remains unaware of the authentication process.

D. AUTHENTICATION SYSTEM MODULES
As illustrated in Fig. 4, the authentication system consists of the MAC Identification Module, Authentication Module, and Flow Control Module.

1) MAC IDENTIFICATION MODULE
The MAC Identification Module is established based on the SNMP protocol. It is responsible for obtaining the ARP and NDP tables from the user’s gateway via SNMP. The ARP and NDP tables provide the mapping of IPv4 and IPv6 to MAC addresses, respectively, enabling the Authentication Module to verify the user information.

2) AUTHENTICATION MODULE
The Authentication Module can utilize a local database, RADIUS, LDAP, or other approaches for user authentication. If a user is authenticated successfully, the user account, IPv4/IPv6 addresses, MAC address, and other information is recorded in the authenticated IP and MAC tables. For an unauthenticated IP address with an authenticated MAC address, this module would utilize the account information used in the MAC authentication, and add the IP address into the authenticated IP table.

3) FLOW CONTROL MODULE
The Flow Control Module determines whether the user is authenticated based on the packet source IP. If the source IP is unauthenticated, the Flow Control Module will contact the Authentication Module to check whether the MAC address of the IP has been authenticated. If yes, the Flow Control Module would add this IP to the authenticated IP table. Otherwise, the user would be redirected to the login page for authentication. If no packet is received from an IP address stored in the authenticated IP table for a certain period, the IP address would be removed.

E. IPV4 AND IPV6 TRAFFIC TRACEABILITY AGAINST SECURITY ATTACKS
Considering the series of steps for providing dual-stack network service mentioned earlier in this section, the traceability of user IPv4 and IPv6 traffic is further enhanced since not only IPv4 but also IPv6 within the system are authenticated. In case of a security incident, the network traffic could be traced immediately by cross-checking authentication and threat logs to find potential attackers based on the source IP. Malicious attacks could then be blocked via the next-generation firewall or the web application firewall. The risk of security attacks through penetrating network vulnerabilities due to the lack of authentication for IPv6 is limited.

IV. IMPLEMENTATION AND PERFORMANCE EVALUATION
The proposed one-time dual-stack authentication mechanism is currently deployed in the authentication system of a
university dormitory network. Under this environment, we perform a series of functional experiments by logging into the authentication system from a personal computer (PC) to verify the feasibility of the proposed one-time authentication architecture within a dual-stack environment. Furthermore, the stability of the system was evaluated by monitoring the system traffic for some time.

1) USER INFORMATION TEST
To test whether the proposed authentication system can obtain relevant user information via SNMP, we used the ipconfig command to obtain the IPv4, IPv6, and MAC addresses of the test PC. Fig. 5 shows that the IPv4 address, IPv6 address, and the physical address (i.e., MAC address) are 140.x.x.245, 2001:288:4001:x:x:x:x:d362, and B8:6B:23:x:x:13, respectively. We then looked up the unauthenticated user list at the system backstage to find relevant login records. As expected, the authentication server obtained the test PC’s information stored in the ARP and NDP tables from the L3 Switch via SNMP. Figs. 6 and 7 illustrate the unauthenticated user list of the test PC’s IPv4 and IPv6 addresses, respectively. The figures show the information of requiring authentication on the server.

2) ONE-TIME AUTHENTICATION TEST
This subsection describes the process of verifying the one-time dual-stack authentication capability of the proposed authentication system to ensure sparing the login for the second protocol after successfully authenticating the first protocol. Following the user information test, the unauthorized test PC was redirected to the login page to pass the authentication by entering the account name and password. The IPv6 authentication logs presented in Fig. 8 indicate that the test PC’s IPv6 and MAC addresses were authenticated via RADIUS. Therefore, when the user tried to initiate another connection via IPv4, the authentication system found that the MAC address had already been authenticated, and there was no need for further authentication, as indicated by the IPv4 authentication logs presented in Fig. 9.

3) MAC AUTHENTICATION TEST
To test whether the system used the stored test PC’s MAC address for authentication, we reconnected the network to obtain a new set of IPv4 and IPv6 addresses and viewed the newly obtained IP and MAC addresses using the ipconfig command. Fig. 10 shows the IPv4 address, IPv6 address, and MAC address are, 140.x.x.218, 2001:288:4001:x:x:x:6bd0,
and B8:6B:23:xx:13, respectively. Since the test PC’s MAC address had been authenticated previously, the newly obtained IPv4 and IPv6 were seamlessly authenticated based on the MAC address, as shown in the IPv4 and IPv6 authentication logs marked in red in Figs. 11 and 12, respectively. There was no need to redirect the user to the login page again, making the user unaware of the authentication process.

4) STABILITY TEST
The proposed authentication system is currently in use in a campus dormitory, and the system has been online for over a year. We browsed the authentication system backstage to select 1-week online user traffic randomly, as showed in Fig. 13. From the figure note that the online user traffic of the authentication system fluctuates around 10,000 users.
per day, and the peak period is usually at midnight. This phenomenon can be explained by the fact that dormitory students tend to surf the Internet during this period. Figure 14 illustrates the SNMP CPU load of the authentication system for the same week as presented on the PRTG network monitor [14]. It shows that the trend of the SNMP CPU load is consistent with that of the online user traffic, i.e., it is higher at midnight because of the increased number of users at this time. In summary, the online users and CPU load remain stable when using the proposed authentication system, indicating that the system provides a practical dual-stack authentication solution for a large network environment.

V. CONCLUSION
The IPv6 protocol has been evolving for many years. Nonetheless, many existing authentication systems lack one-time authentication mechanisms in IPv4/IPv6 dual-stack network environments. This paper reviews the existing authentication technologies and mechanisms of various authentication methods. Based on the presented surveys, the existing authentication systems would require a faster and more effective one-time authentication scheme when IPv6 gradually becomes popular. In many cases, the authentications of IPv4 and IPv6 are considered separately, and some applications even fail to authenticate IPv6. Thus, simultaneously authenticating IPv4 and IPv6 becomes a highly demanding functionality when providing network services.

This work implements the one-time authentication mechanism based on SNMP that can acquire the user’s IPv4, IPv6, and MAC addresses from the ARP and NDP tables and utilizes the MAC address for authentication. The proposed mechanism provides a functioning solution to resolve problems related to IPv6 authentication. For future improvement, artificial intelligence is a promising tool to perform log analysis and build predictive models for detecting abnormal dual-stack traffic proactively. Furthermore, an automated intrusion detection prevention system can be deployed to prevent malicious network behaviors by integrating the proposed solution with the auto-blocking mechanism [15], [16].

ACKNOWLEDGMENT
The authors would like to thank UGuard Technologies for their help. This work benefits greatly from their insight and expertise. This article was presented in part at the Fourth International Symposium on Mobile Internet Security, Taichung, Taiwan, October 2019.

REFERENCES
[1] J.-C. Liu, Y.-Q. Ke, Y.-C. Kao, S.-C. Tsai, and Y.-B. Lin, “A dual-stack authentication mechanism through SNMP,” in Proc. 4th Int. Symp. Mobile Internet Secur., 2019, pp. 1–13.
[2] Google IPv6 Adoption Statistics. Accessed: Sep. 6, 2019. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html
[3] Taiwan IPv6 Global Ranking. Accessed: Sep. 6, 2019. [Online]. Available: https://ipv6now.twnic.net.tw/ipv6/index.html
[4] TWNIC. (2012). IPv6 Upgrade Implementation Technical Manual. [Online]. Available: https://ipv6now.twnic.net.tw/ipv6/index.html
[5] M. Patrick. (2001). RFC 3046: DHCP Relay Agent Information Option. [Online]. Available: https://tools.ietf.org/html/rfc3046

[6] S. Thomson. (2007). RFC 4862: IPv6 Stateless Address Autoconfiguration. [Online]. Available: https://tools.ietf.org/html/rfc4862

[7] Y.-C. Kao, Y.-C. Chang, and R.-S. Chang, “EZ-Net BYOD service management in campus wireless networks,” J. Internet Technol., vol. 18, no. 4, pp. 907–917, 2017.

[8] Y. Lu, M. Wang, and P. Huang, “An SDN-based authentication mechanism for securing neighbor discovery protocol in IPv6,” Secur. Commun. Netw., vol. 2017, pp. 1–9, 2017.

[9] X.-Y. Huang, Z. Chen, Y.-F. Hu, and R. Cai, “Single login authentication for users with multiple IPv4/IPv6 addresses,” U.S. Patent 9 467 456 B2, Oct. 11, 2016.

[10] J. H. Bennett, III, J. R. Breau, B. B. Hirschman, T. D. Nebergall, and F. C. Rogers, “Optimizing device authentication by discovering Internet protocol version authorizations,” U.S. Patent 8 151 325 B1, Apr. 3, 2012.

[11] S. Sanguanpong and K. Koh-Arsa, “A design and implementation of dual-stack aware authentication system for enterprise captive portal,” in Proc. 9th Int. Conf. Netw. Service Manage. (CNSM), Oct. 2013, pp. 118–121.

[12] T. Lin, “Method and apparatus for dual stack access,” U.S. Patent 9 094 264 B2, Jul. 28, 2015.

[13] D.-J. Wang, Design and Implementation of Authentication System for IPv4/IPv6 Dual Stack Hosts. Beijing, China: China Academic Journal Electronic Publishing House, 2017.

[14] PRTG Network Monitor. Accessed: Sep. 26, 2019. [Online]. Available: https://www.paessler.com/prtg

[15] S.-J. Fu, H.-W. Hsu, Y.-C. Kao, S.-C. Tsai, and C.-C. Tseng, “An auto-blocking mechanism for firewall service,” in Proc. IEEE Conf. Dependable Secure Comput., Aug. 2017, pp. 531–532.

[16] Y.-C. Kao, J.-C. Liu, Y.-H. Wang, Y.-H. Chu, S.-C. Tsai, and Y.-B. Lin, “Automatic blocking mechanism for information security with SDN,” J. Internet Service Inf. Secur., vol. 9, no. 1, pp. 60–73, 2019.