# A Dual-Stack Authentication Mechanism Through SNMP

Jui-Chun Liu[1]*, Yi-Quan Ke[1], Yi-Chih Kao[1], Shi-Chun Tsai[2], and Yi-Bing Lin[2]
[1]*Information Technology Service Center, National Chiao Tung University, Hsinchu, Taiwan*
{g0737, h0631, ykao}@nctu.edu.tw
[2]*Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan*
{sctsai, liny}@cs.nctu.edu.tw

Received: November 1, 2019; Accepted: December 7, 2019; Published: December 31, 2019

**Abstract**

The rapid development of IoT (Internet of Things) has further promoted the deployment and application of IPv6. The huge IP addresses requirements of the IoT sensors will also contribute to the popularity of IPv6. Therefore, the importance of IPv6 has become a trend. However, the design of IPv6 is incompatible with that of IPv4, which increases the difficulty in integration. In order to bridge the gap between these two heterogeneous protocols, the IETF has proposed numerous transitioning mechanisms to attain the compatibility of IPv4 and IPv6. The most common techniques are dual-stack, tunneling and translation. Before IPv6 completely takes over IPv4, these two heterogeneous protocols still need to coexist continually for a long period of time. However, we found that the existing captive portal authentication systems generally do not support IPv4/IPv6 dual-stack authentication, and furthermore lack of one-off dual-stack authentication solutions. Upgrading the authentication system has become an urgent problem to be addressed. This research presents a one-off authentication architecture for the coexisting IPv4 and IPv6 with the Simple Network Management Protocol (SNMP) to gain user MAC address and IP address for identity authentication. It resolves the inconvenience that IPv4 and IPv6 need to be authenticated separately, and effectively improves the compatibility of the authentication system. Lastly, we successfully verify the feasibility and stability in a dormitory environment.

**Keywords**: IPv6, Dual-Stack, Authentication, SNMP

## 1 Introduction

The exhaustion of IPv4 addresses is reality. To keep network services running, the introduction of IPv6 addresses is an inevitable result. As the successor of IPv4, IPv6 increases the existing address length of IPv4 by 4 times, expanding from the current 32 bits (4 bytes) to 128 bits (16bytes). As a result, IPv6 has $3.4 \times 10^{38}$ address spaces, a significant increase from $1.9 \times 10^{9}$ address space of IPv4, providing a huge amount of IP addresses for exploitation. In addition, IPv6 had 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 (AH) in the header, the integrity and non-repudiation of packets transmission is ensured by Encapsulating Security Payload (ESP) on packets encryption to enhance confidentiality and keep transmitted contents from being eavesdropped by malicious attackers. Another important feature of IPsec is the provision of Virtual Private Network (VPN) functionality, enabling a more secure and reliable VPN in IPv6. On the other hand, QoS uses the Flow Label field in the IPv6 header to meet the

*Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 10(4):31-45, Dec. 2019
DOI:*10.22667/JOWUA.2019.12.31.031*

*Corresponding author: Information Technology Service Center, National Chiao Tung University, 1001 University Road, 30010, Hsinchu, Taiwan, Tel: +886-988-835-826

low latency requirements of multimedia applications (e.g., VoIP, video, etc.) and provide highly efficient network transmission quality.

The rapid development of digitization has resulted in a variety of intellectual end devices in various of applications. A large number of applications, such as mobile devices, sensors, self-driving cars and wearable devices, had significantly increased the demand of massive amount of IP addresses [6]. With 6LoWPAN [12], a low-power wireless network protocol suitable for IoT applications that is in charge of the packets transmission between IEEE 802.15.4 and IPv6 [14], IoT and IPv6 are gradually integrated.

IPv6 has been widely used nowadays, according to the statistics report from Google [1], the global IPv6 deployment and adoption rate has reached 25% in 2018. Meanwhile, according to the data from Taiwan Network Information Center (TWNIC) [3], the IPv6 deployment and adoption rate of Taiwan has increased from 0.38% (67th place in global ranking) in November 2017 to 34.93% (7th place in global ranking) in January 2019.

Currently, most network hardware and software systems are operating under the IPv4 protocol. 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 all these network components above often make users hesitate.

IPv6 is expected to completely replace the role of IPv4 on the Internet, but before this moment arrives, there is still a long period of time that IPv4 and IPv6 will coexist. Hence, several IPv4/IPv6 transitioning mechanisms had been developed. The most common ones are dual-stack, tunneling and translation. Since tunneling and translation have performance bottleneck [2], they can only be used as short-term solutions. Only the dual-stack approach can gradually evolve from IPv4 dominant network to IPv4/IPv6 dual-stack network where these both coexist, then finally reach purely IPv6-based network. Therefore, our study is based on the dual-stack technique.

With the continuous development of IPv6, effectively authenticating the identity of users has become a new issue. In a dual-stack network environment, most captive portals can only authenticate one kind of protocol, either IPv4 or IPv6, one by a time. This is the reason why this kind of authentication systems will carry out authentication twice at user's IPv4 and IPv6 respectively. That is, after IPv4 has been authenticated, it has to be authenticated again if one need to access IPv6 applications. Similarly, when IPv6 has been authenticated, it has to be authenticated once again if one need to access IPv4 applications. Such inconvenience will deter users from migrating to IPv6. Even worse, some systems are unable to authenticate IPv6 addresses, resulting to security concerns. Therefore, we propose a dual-stack authentication mechanism under a IPv4/IPv6 coexistence dual-stack environment that achieves one-time authentication with efficiency and convenience.

This paper is organized as follows. Section 2 provides the literature review related to the IPv4/IPv6 dual-stack authentication mechanism; Section 3 describes the proposed architecture and the process of the authentication mechanism in detail, as well as its improvements over existing works; Section 4 presents the authentication test and stability test of this mechanism; and finally, section 5 contains the conclusion and future work.

## 2 Background and Related Works

This section overviews existing works related to IPv4/IPv6 transitioning mechanism, MAC authentication and dual-stack authentication mechanism.

## 2.1 IPv4/IPv6 Transitioning Mechanism

The commonly used IPv4/IPv6 transitioning mechanisms include dual-stack, tunneling and translation. Dual-stack is the most popular and widely used transitioning mechanism which turns an IPv4-capable device into one supporting IPv4 and IPv6 simultaneously. A dual-stack-capable device not only enables IPv4 and IPv6 to coexist, but also features interoperability and backwards compatibility. Tunneling encapsulates an IPv4 header outside the IPv6 packet, allowing IPv6-capable network devices at two ends communicating through IPv4 tunnel, providing IPv6 virtual connections over IPv4 physical network. Similar to Network Address Translation (NAT), translation utilizes the router or default gateway at IPv4 or IPv6 border in responsible for converting the IPv4 header to the IPv6 header or vice versa, allowing IPv4 and IPv6 network devices to communicate with each other.

## 2.2 MAC Authentication

MAC authentication the approach that authenticates devices based on MAC address which must matches with the predefined IP address. Kao et al. [9] summarized the specific process of MAC authentication as follows: If a user device fails to be authenticated by the RADIUS after connecting to the Internet, it will be redirected to captive portal where the user has to enter their credentials, which together with the MAC address will be stored in the database. Next time, when the user connects to the Internet via the same device, the user device will automatically pass the identity authentication by checking with the MAC address stored in the database.

The authentication mechanism based on Software-Defined Networking (SDN) proposed by Lu et al. [11] contains an authentication-table module which maintains a sheet to store the collected users' device information. The sheet is indexed by MAC address to avoid duplicate entries. The verification module parses all packet-in ICMPv6 packets to filter out NDP packets to check whether the source MAC address and source IPv6 match the information stored in the authentication-table. Although this study exploits MAC address as the key value, the same as our proposed mechanism meant to be, it only proposed authentication mechanism for IPv6 and did not describe the authentication mechanism in the circumstance of IPv4/IPv6 dual-stack.

## 2.3 Dual-Stack Authentication Mechanism

As mentioned by Huang et al. [8], most of users may access multiple network resources during the course of a work session, so the user devices have to authenticate via separate login procedures for each IP address to gain access of one or more network resources. The productivity of that user can be decreased significantly as the user has to perform many separate authentications. Hence our research intended to discuss several dual-stack authentication mechanisms proposed by different authors, to seek for the best technique that solves this issue.

The framework proposed by Bennett III et al. [7] authenticates devices through discovering user devices IP version to determine whether it is 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 necessary steps to authenticate IPv4, thus unnecessary resources will not be consumed to authenticate user device's IPv6, and vice versa. However, their solution did not perform testing in actual environmental, and there were performance concerns when applied to complex network environments.

Sanguanpong et al. [13] proposed a mechanism to avoid duplicate authentication under dual-stack architecture, called Dual Address Discovery (DAD). By embedding two image tags in the login page, where one of the DNS forward mapping to IPv4 address, and the other mapping to IPv6 address, we can now bind two separate protocols together with identical hash code. Once the user has both IPv4 and

IPv6, the authentication server can associate user' IPv4 and IPv6 addresses with the hash code, thereby authenticating both protocols at one time. Such an approach can effectively save the time wasted by repeated authentication, and the architecture is relatively simple and easy to deploy, but there are still some problems to be solved. For examples, users need to have both IPv4 and IPv6 addresses during authentication process to achieve one-off authentication. If users complete the authentication in a pure IPv4 environment and then converts to a dual-stack environment, authentication must be gone through again in order to let the authentication server to associate IPv4 and IPv6. The research by Sanguanpong et al. did not elaborate on the system architecture of the tested environment, nor did it verify and evaluate the performance, stability and feasibility in the real network environment.

In the method designed by Lin [10], the authentication system controls the address allocation process of the second IP address after the first IP address is authenticated. Then the authentication system stores both IPv4 and IPv6 addresses and other information in the user information table, and manage dual-stack user's network access according to control policy configured through stored information. This solves the problem that any randomly configured address can access the service through the network device without authentication. For example, when an IPv4 user is authenticated by the portal, the user information is added to the database, and the Router Advertisement is sent to the user to notify the user of the IPv6 address configuration method. On the other hand, when the user's IPv6 is authenticated by the portal, the user information is added to the database, and a DHCPv4 discovery message is sent to the user to notify the user of the IPv4 address configuration method, thereby achieving the access control of the dual-stack user. However, the Router Advertisement proposed by Lin must be placed in the lower layer (Gateway) of the network architecture. General network does not have such environment and resources to implement a large amount of authentication devices. Therefore, this method is not suitable for centralized network environments that are only managed by the upper layer-3 authentication server.

Wang [4] obtained the IPv4 and IP6 association of the user by parsing DHCP packets. In an IPv4 environment, the MAC address in the DHCP packet can be used to associate the IPv4 address of the user. Meanwhile, there is DHCP Unique Identifier (DUID) that identifies the DHCPv6 device in the DHCPv6 packet, thus binding the user DUID with IPv6 address. In order to attain IPv4/IPv6 dual-stack authentication at one-time, the DNS server is responsible for redirecting all requests of the user to the authenticated portal page when the user obtains the IP address. If an unauthenticated user uses certain protocol to access the portal, it will be redirected to portal login page while carrying an encrypted message, and the Javascript code will actively trigger the user to access another portal login page with the other protocol carrying the same encrypted message as above. When the portal obtains user's IPv4 address and IPv6 address at the same time, the user's IPv4/IPv6 binding is achieved.

We summarized dual-stack authentication mechanisms proposed by the above authors in Table 1. Although some of the authentication mechanisms can achieve authentication when IPv4 and IPv6 coexist, there are still several limitations and difficulties while in use, also lack of flexibility in operation. For example, Lin's solution relies on Router Advertisement, which must have a device supporting RA. It is not suitable for a network environment that is managed centrally only by the upper L3 authentication server. Besides, Sanguangpong et al. and Wang both adopt the method of embedding the same hash code, which must have both IPv4 and IPv6 addresses in present while conducting user authentication to achieve one-off authentication. The flexibility appears to be limited.

## 3 Proposed Framework

As pointed out in [4] that the traditional methods of binding user MAC addresses and IP addresses for authentication have several problems in the dual-stack environment. First of all, when the authentication equipment is deployed in the environment between the layer-3 switch (L3 switch) and internal network,

Table 1: Summary of dual-stack authentication mechanisms

| Author | Solution | Pro | Cons |
|---|---|---|---|
| Bennett III et al. [7] | Determine IP version of user and check whether it is authorized to access data via IPv4, IPv6, or both. | Only trigger necessary steps for authentication without authenticating both IPv4 and IPv6. | There is no field trial or test in functioning network environment. Performance issue exists. |
| Sanguanpong et al. [13] | Bind two image tags of IPv4 and IPv6 through identical hash code for further matching. | Effectively reduce repeated authentication. The structure is relatively simple and easy to deploy. | Users must have IPv4 and IPv6 addresses simultaneously while authenticating to achieve one-off authentication. |
| Lin et al. [10] | After the first IP address is authenticated, the system will control and monitor the process of the second IP address configuration. | Avoid any randomly configured IP address to access the service through the network device without authentication. | Not applicable to network environments that are only managed centrally by the upper layer-3 authentication server. |
| Wang et al. [4] | Use MAC and DUID to correspond to the user's IPv4 and IPv6 respectively, and then bind the above information. | IP addresses binding only relies on browser's JavaScript code and does not require other plug-ins or software. | Users have to equip with IPv4 and IPv6 addresses simultaneously to achieve one-off authentication. |

user's MAC address may be dropped by the routing equipment in between, and thus fails to create an IPv4/IPv6 association of the same user. Secondly, if the stateful autoconfiguration is adopted in the DHCPv6 address configuring process, the message passed through the DHCPv6 Relay does not contain MAC address information, and no IPv4/IPv6 association is established.

This study proposes a cross-layer-3 MAC authentication solution that is suitable for the dual-stack environment by exploiting the authentication server (Auth server) to query the L3 switch periodically for the Address Resolution Protocol (ARP) table, and the Neighbor Discovery Protocol (NDP) table through Simple Network Management Protocol (SNMP) to obtain the MAC address and IP address of the user devices stored in the L3 switch. When the L3 switch receives the request message, it will send its ARP table and NDP table back to the Auth server. Then the Auth server compares the obtained content with the user's IP address and its MAC address, if the MAC address matches the information in the Auth server, the user is authenticated successful. If the MAC address does not match, the authentication fails. The cross-layer-3 MAC authentication based on SNMP solves the problem that the upper-layer authentication device of the L3 switch cannot read the user MAC address. In this way, a flexible and easy to deploy dual-stack authentication mechanism is achieved.

### 3.1 Traditional Authentication Mechanism

In the traditional authentication system, a user attempts to initiate the first HTTP connection through IPv4 (Figure 1(a)). The Auth server finds that the user has not been authenticated according to the packet source IP (Figure 1(b)). The unauthenticated user will be redirected to the authentication page

(Figure 1(c)), and the user will be authenticated after entering the account and password (Figure 1(d)). Then the Auth server will recognize the user as authenticated (Figure 1(e)), the user can now use the network service through IPv4 (Figure 1(f)). After completing the IPv4 authentication, the user attempts to initiate the connection through IPv6 (Figure 1(g)). The Auth server finds that the user has not been authenticated according to the packet source IP (Figure 1(h)). The unauthenticated user will be redirected to the authentication page again (Figure 1(i)), and the user has to re-enter the account and password for authentication (Figure 1(j)), then the Auth server will recognize the user as authenticated (Figure 1(k)). Now user can use the network service through IPv6 (Figure 1(l)). Similarly, if the user first passes IPv6 authentication, the user still needs to authenticate again when using IPv4.

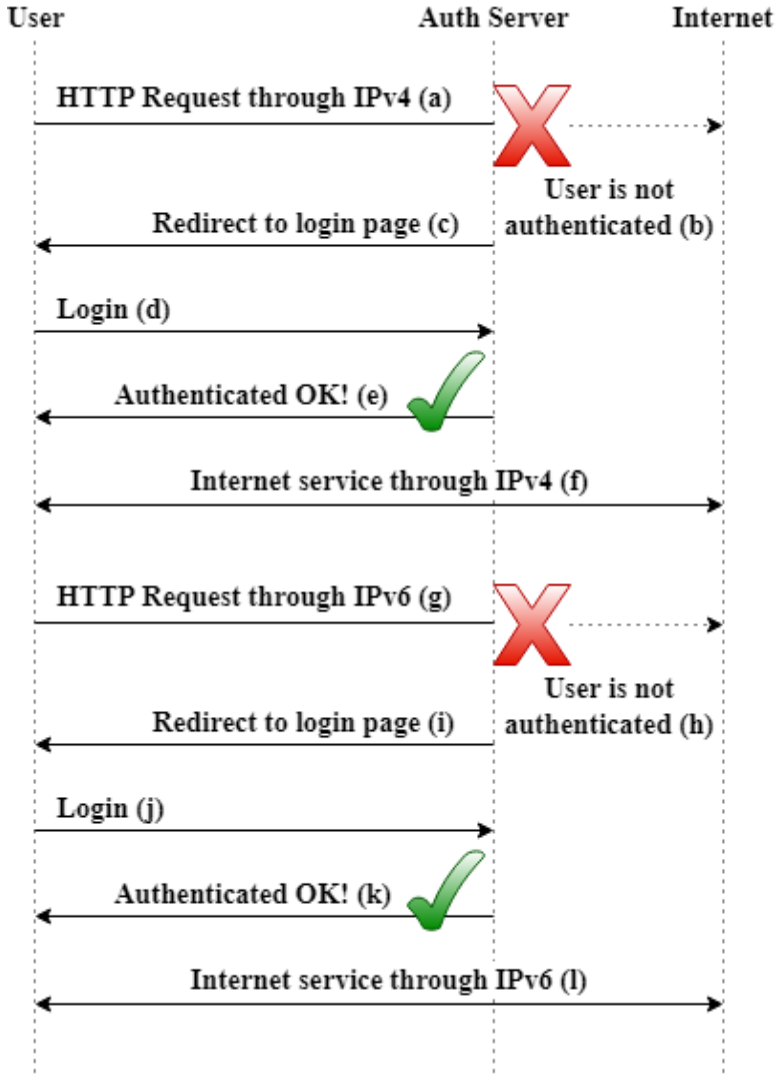


Figure 1: Flow chart of traditional authentication mechanism

## 3.2 Proposed Authentication Mechanism

In the authentication mechanism proposed by this study, the L3 switch records the underlying user information on the IPv4 ARP table and the IPv6 NDP table (Figure 2(a)). The Auth server can obtain this information from the L3 switch through SNMP (Figure 2(b)). When a user attempts to initiate the first

HTTP connection through IPv4 (Figure 2(c)). The Auth server compares the packet source IP with the ARP table and obtains the MAC address of the user and finds that the MAC address has not been authenticated (Figure 2(d)). Users who have not been authenticated will be redirected to the authentication page (Figure 2(e)), then the user is authenticated after entering the account and password (Figure 2(f)). The Auth server records this MAC address as authenticated (Figure 2(g)), now the user can use the network service via IPv4 (Figure 2(h)). After completing the IPv4 authentication, if the user attempts to use IPv6 to initiate the connection (Figure 2(i)), the Auth server compares the packet source IP with the NDP table to obtain the MAC address of the user, and finds that the MAC address has been authenticated. Therefore, it will not block the IPv6 packet (Figure 2(j)) and the user can use the network service over IPv6 without having to authenticate (Figure 2(k)) again. Similarly, if a user first passes IPv6 authentication, the Auth server can still identify whether the IPv4 address has passed the authentication through recorded MAC address and ARP table. There is no need to authenticate again via IPv4.

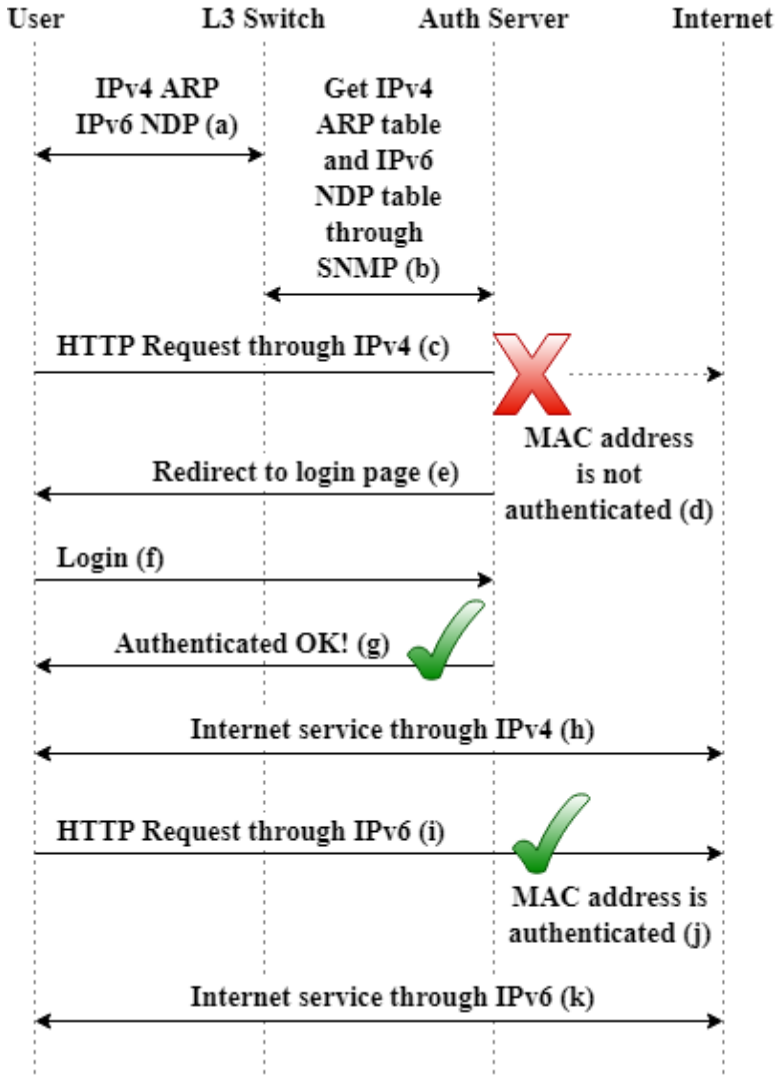


Figure 2: Flow chart of proposed authentication mechanism

The traditional authentication architecture requires separate authentication for both IPv4 and IPv6, some systems even authenticate only either IPv4 or IPv6, which is vulnerable to security attacks. In

contrast, the authentication mechanism proposed in this study first uses SNMP to obtain the user identity information from the ARP table and the NDP table, and then uses the recorded MAC address to authenticate the user's identity and completes the authentication of the user's IPv4/IPv6 at one-time. When the connection is initiated again by another protocol, the second authentication is not required, achieving authentication without user awareness.

### 3.3 Authentication System Modules

Figure 3 shows the diagram of the authentication system modules. The MAC Identification Module is established based on the SNMP protocol and is responsible for obtaining the ARP table and the NDP table from the user's gateway through SNMP. The ARP table and the NDP table provide the mapping of IPv4 and IPv6 to MAC address respectively, enabling the Authentication Module to verify user information.

The Authentication Module can utilize local database, RADIUS, LDAP or other approaches for user authentication. If authenticated successfully, user account, IPv4/IPv6 addresses, MAC address and other information will be recorded in the authenticated IP table and the authenticated MAC table. If an unauthenticated IP address has an authenticated MAC address stored in the authenticated MAC table, the authentication module will use the account that was used at previous MAC authentication as the account of the unauthenticated IP address, then add the user account into the authenticated IP table.

The Flow Control Module determines whether the user is authenticated based on the packet source IP. If the source IP is an unauthenticated IP, the Flow Control Module contacts with the Authentication Module to check whether the MAC address of the IP had been authenticated. If the MAC address had already been authenticated, the Flow Control Module will add this IP to the authenticated IP table. Otherwise, the user will be redirected to the authentication page for authentication. If no packet is received from an IP address that is on the authenticated IP table for a certain period of time, the IP will be removed.

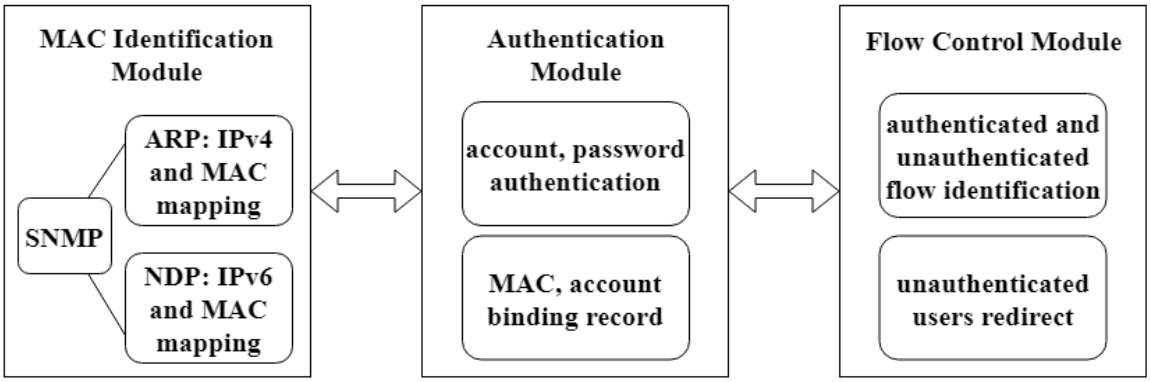


Figure 3: Diagram of the authentication system modules

## 4 Implementation and Performance Evaluation

In order to verify the feasibility of the one-off authentication architecture proposed in this study within the dual-stack environment, we establish the one-off authentication system network environment in our university dormitory. We experiment with a series of functional testings by logging into the authentication system using test PC. In addition, we verify the stability of the system by monitoring system traffic for a period of time.

### 4.1 Testing Environment

The main components of the proposed authentication architecture include a Core Router, an Authentication Server with database (Auth server), an Internal Router, Layer 3 Switches (L3 switches), Layer 2 Switches (L2 switches) and End user devices. In this architecture, the Core router (Figure 4(a)) is the gateway of the entire architecture for external connection; the Auth server (Figure 4(b)) is responsible for determining whether underlying traffic is from the authenticated user; the Internal router (Figure 4(c)) is responsible for collecting the cables from the L3 switches (Figure 4(d)); L3 switches are the gateway for each dormitory network, distributing network cables to each rooms' network ports through L2 switches (Figure 4(e)) to provide End user devices (Figure 4(f)) network service.

Instead of connecting all the L3 switches directly to the Auth server to connect the backbone network, our proposed architecture utilizes a router to accommodate each L3 switch traffic. Thus, the Auth server only needs manage upward and downward network interfaces, making the network architecture relatively simple and easier to manage. In this framework, the L3 switch as a gateway itself maintains IPv4 address and MAC address mapping ARP table as well as a IPv6 address and MAC address mapping NDP table. Since the user's MAC address is unique and fixed, the L3 switch will have information about the IPv4 addresses, IPv6 addresses, and MAC addresses. Based on the above conditions, Auth server obtains user information through the SNMP protocol and we implement it as a MAC-based authentication mechanism.

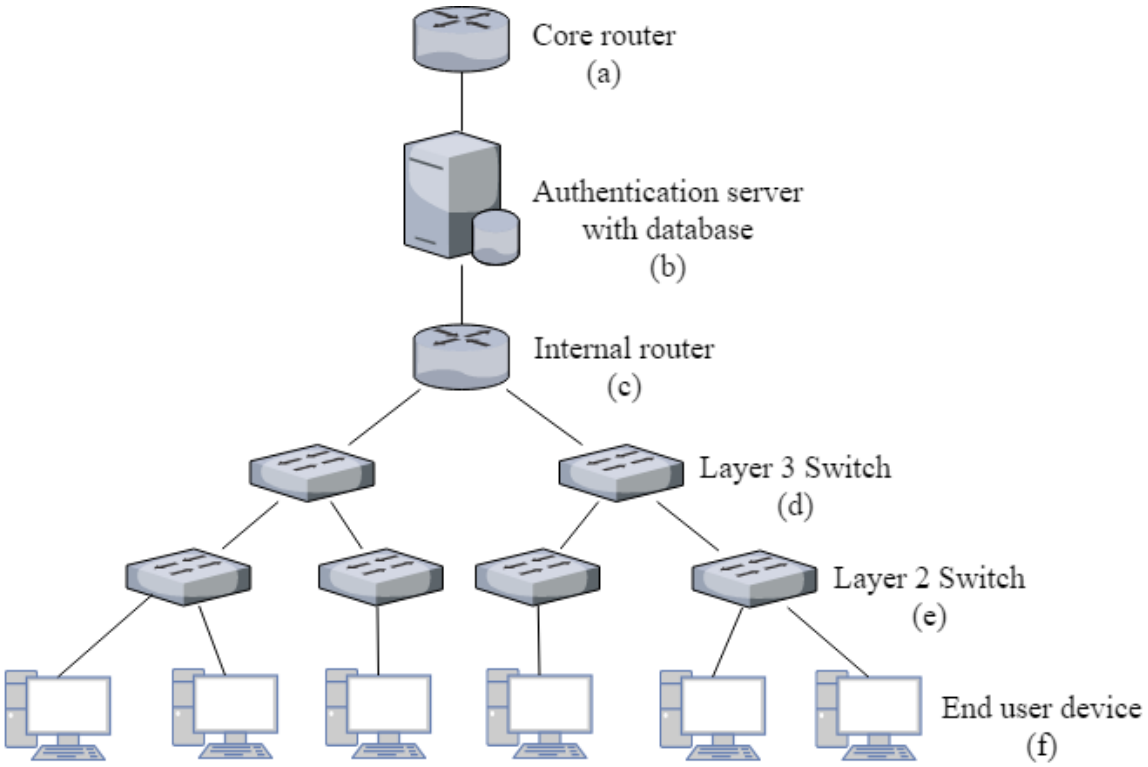


Figure 4: Authentication system architecture diagram

### 4.2 User Information Test

In order to test whether the proposed authentication architecture can obtain relevant user information through SNMP, we first use ipconfig command to get the IPv4/IPv6 addresses and MAC address of the

test PC, as shown in Table 2. We then look up the unauthenticated users list at system backstage and find relevant records on the list. Table 3 and Table 4 illustrate the unauthenticated users list of test PC's IPv4 and IPv6 respectively, which indicate the reason for authentication failure is the need of server authentication.

Table 2: User Information Test

| |
|---|
| C:\Users\Test1>ipconfig /all |
| IPv6 Address ..... : 2001:288:4001:x:x:x:x:d362 |
| IPv4 Address ..... : 140.xxx.xxx.245 |
| Physical Address ..... : B8:6B:23:xx:xx:13 |

Table 3: Unauthenticated IPv4 users list of User Information Test

| No. | IP Address / MAC Address | Time | Reason for authentication failure |
|---|---|---|---|
| 1 | 140.xxx.xxx.245 / b8:6b:23:xx:xx:13 | 16:15:31 | Require Server Authentication |

Table 4: Unauthenticated IPv6 users list of User Information Test

| No. | IP Address / MAC Address | Time | Reason for authentication failure |
|---|---|---|---|
| 1 | 2001:288:4001:x:x:x:x:d362 / b8:6b:23:xx:xx:13 | 16:15:36 | Require Server Authentication |

### 4.3 One-off Authentication Test

In this section, we verify the one-off authentication capability of the proposed system to ensure that the authentication for the second protocol will not be launched after the initial authentication for the first protocol has completed. Following the User Information Test, unauthorized user will be redirected to the authentication page to pass the authentication by entering account and password. As shown in Table 5, the IPv6 authentication logs presents that the test PC's IPv6 and the MAC address are authenticated via RADIUS. Therefore, when user tries to initiate another connection via IPv4, the authentication system will find that its MAC address has already been authenticated, and there is no need for further authentication, as shown in Table 6. At this point, we can find both IPv4 and IPv6 of the test PC in the authenticated user list from Table 7.

Table 5: IPv6 authentication logs of One-off Authentication Test

| No. | User/Group | IP Address / MAC Address | Time | Authenticated by |
|---|---|---|---|---|
| 1 | Test1/Dorm | 2001:288:4001:x:x:x:x:d362 / b8:6b:23:xx:xx:13 | 16:21:55 | RADIUS |

Table 6: IPv4 authentication logs of One-off Authentication Test

| No. | User/Group | IP Address / MAC Address | Time | Authenticated by |
|---|---|---|---|---|
| 1 | Test1/Dorm | 140.xxx.xxx.245 / b8:6b:23:xx:xx:13 | 16:22:13 | MAC |

Table 7: Authenticated users list of One-off Authentication Test

| No. | User/Group | IP Address / MAC Address | Time |
|---|---|---|---|
| 1 | Test1/Dorm | 140.xxx.xxx.245 / b8:6b:23:xx:xx:13 | 16:15:31 |
| 2 | Test1/Dorm | 2001:288:4001:x:x:x:x:d362 / b8:6b:23:xx:xx:13 | 16:15:36 |

## 4.4 MAC Authentication Test

In order to test whether the system is actually using the stored user MAC address for authentication, we reconnect the network to obtain a new set of IP addresses, and view the obtained IPv4/IPv6 addresses and MAC address through ipconfig command as illustrated in Table 8. Since this MAC address has been authenticated by the authentication system, the IPv4 and IPv6 of the test PC are directly authenticated through the MAC address, as shown in Table 9 and Table 10. There is no need to enter the authentication page again to log in, achieving authentication without user awareness. We can find both IPv4 and IPv6 of the test PC in the authenticated user list from Table 11.

Table 8: Test PC information of MAC Authentication Test

```
C:\Users\Test1>ipconfig /all
IPv6 Address ..... : 2001:288:4001:x:x:x:x:6bd0
IPv4 Address ..... : 140.xxx.xxx.218
Physical Address ..... : B8:6B:23:xx:xx:13
```

Table 9: IPv6 authentication logs of MAC Authentication Test

| No. | User/Group | IP Address / MAC Address | Time | Authenticated by |
|---|---|---|---|---|
| 1 | Test1/Dorm | 2001:288:4001:x:x:x:x:6bd0 / b8:6b:23:xx:xx:13 | 16:28:36 | MAC |
| 2 | Test1/Dorm | 2001:288:4001:x:x:x:x:d362 / b8:6b:23:xx:xx:13 | 16:21:55 | RADIUS |

Table 10: IPv4 authentication logs of MAC Authentication Test

| No. | User/Group | IP Address / MAC Address | Time | Authenticated by |
|---|---|---|---|---|
| 1 | Test1/Dorm | 140.xxx.xxx.218 / b8:6b:23:xx:xx:13 | 16:27:54 | MAC |
| 2 | Test1/Dorm | 140.xxx.xxx.245 / b8:6b:23:xx:xx:13 | 16:22:13 | MAC |

Table 11: Authenticated users lists of MAC Authentication Test

| No. | User/Group | IP Address / MAC Address | Time |
|---|---|---|---|
| 1 | Test1/Dorm | 140.xxx.xxx.218 / b8:6b:23:xx:xx:13 | 16:27:27 |
| 2 | Test1/Dorm | 2001:288:4001:x:x:x:x:6bd0 / b8:6b:23:xx:xx:13 | 16:28:08 |

## 4.5 Stability Test

There are about 4,000 online users in the campus dormitory authentication system each day, and the system has been online for over a year. We browse the authentication system backstage to randomly select any 7-day online user traffic, as showed in Figure 5. The number of online users maintains in

stability. We observe the SNMP CPU Load on PRTG network monitor [5] by randomly selecting 7 days. According to Figure 6, the CPU loading appears to be in a normal and stable status.

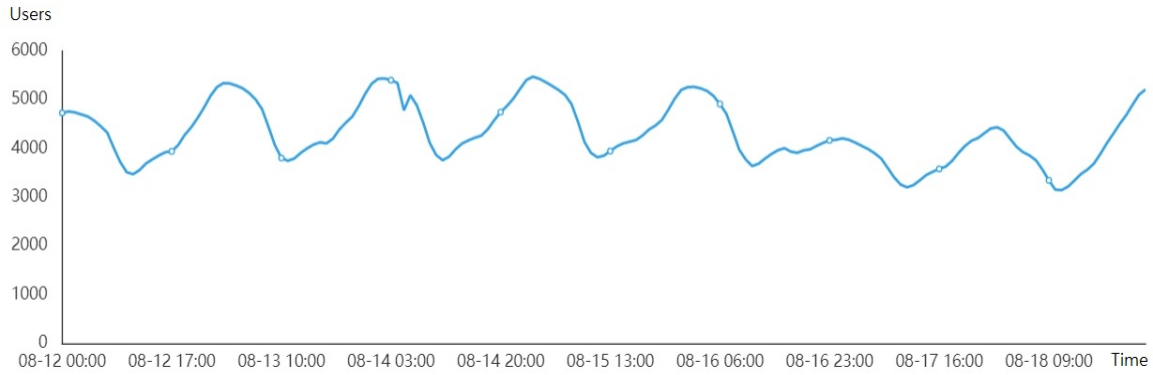


Figure 5: Online user traffic


Figure 6: SNMP CPU load

## 5 Conclusion and Future Work

The promotion of IPv6 has been going on for many years, but plenty of researchers found that most existing authentication systems rarely do one-off authentication for IPv4/IPv6 dual-stack. This paper inspects existing authentication technologies and mechanisms of various authentication methods. We found that the authentication system needs a faster and more effective one-off authentication scheme while IPv6 is gradually popularized. For example, under the environment of a university campus network, IPv4 and IPv6 are basically two authentication methods, and in many applications IPv6 is not even authenticated. Thus simultaneously authenticating IPv4/IPv6 dual-stack becomes a demanding functionality for campus network services.

This work implements a one-off authentication method based on SNMP, which can acquire user IPv4/IPv6 and MAC addresses from the ARP table and the NDP table, then utilize MAC address for authentication. Once authenticated, the system can recognize the MAC address and achieve automatic authentication. With the booming of IoT applications, IPv6 will become even more popular. Our work provides a functioning solution on resolving related problems. To meet tremendous potential applications, we expect to reinforce the robustness of our system architecture. We leave it as a future work.

## Acknowledgements

This research 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) of Taiwan.

## References

[1] "Google ipv6 adoption statistics," https://www.google.com/intl/en/ipv6/statistics.html [Online; accessed on December 15, 2019].

[2] "Ipv6 upgrade implementation technical manual," https://www.gsnv6.tw/docu/SOP/01.IPv6_SOP_IP_Network.pdf [Online; accessed on December 15, 2019].

[3] "Taiwan ipv6 global ranking," https://ipv6now.twnic.net.tw/ipv6/index.html [Online; accessed on December 15, 2019].

[4] "Design and implementation of authentication system for ipv4/ipv6 dual stack hosts." http://gb.oversea.cnki.net/KCMS/detail/detail.aspx?filename=1017290741.nh&dbcode=CMFD&dbname=CMFD2018 [Online; accessed on December 15, 2019], 2014.

[5] "Prtg network monitor," https://www.paessler.com/prtg [Online; accessed on December 15, 2019], 2019.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, June 2015.

[7] J. H. Bennett, I. J. R. Breau, B. B. Hirschman, T. D. Nebergall, and F. C. Rogers, "Optimizing device authentication by discovering internet protocol version authorizations," https://patents.google.com/patent/US8151325 [Online; accessed on December 15, 2019], 2012, u.S. Patent No. 8,151,325.B1.

[8] X. Huang, Z. Chen, Y. Hu, and R. Cai, "Single login authentication for users with multiple ipv4/ipv6 addresses," https://patents.google.com/patent/US9467456B2/ [Online; accessed on December 15, 2019], 2016, u.S. Patent No. 9,467,456.B2.

[9] Y.-C. Kao, Y.-C. Chang, and R.-S. Chang, "Ez-net byod service management in campus wireless networks," *Journal of Internet Technology*, vol. 18, no. 4, pp. 907–917, July 2017.

[10] T. Lin, "Method and apparatus for dual stack access," https://patents.google.com/patent/US9094264B2/en [Online; accessed on December 15, 2019], 2015, u.S. Patent No. 9,094,264.B2.

[11] Y. Lu, M. Wang, and P. Huang, "An sdn-based authentication mechanism for securing neighbor discovery protocol in ipv6," *Security and Communication Networks*, vol. 2017, pp. 1–9, January 2017.

[12] G. Mulligan, "The 6lowpan architecture," in *Proc. of the 4th workshop on Embedded networked sensors (EmNets'07), Cork, Ireland*. ACM, June 2007, pp. 78–82.

[13] S. Sanguanpong and K. Koht-Arsa, "A design and implementation of dual-stack aware authentication system for enterprise captive portal," in *Proc. of the 9th International Conference on Network and Service Management (CNSM'13), Zurich, Switzerland*. IEEE, October 2013, pp. 118–121.

[14] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 22–32, February 2014.

## Author Biography

**Jui-Chun Liu** rececived his B.S degrees in Management of Information System from National Chung Hsing University in 2018. He is now with Information Technology and Service Center at National Chiao Tung University. His research interests are network communication and computer network.

**Yi-Quan Ke** rececived his B.S degrees in Communications Engineering from Feng Chia University in 2016. He is now with Information Technology and Service Center at National Chiao Tung University. His research interests include network communication and information security.

**Yi-Chih Kao** is currently the director of the Network and System Division of the Information Technology Service Center at National Chiao Tung University (NCTU). He received his Ph.D. degree in Industrial Engineering and Management from NCTU. His research interests include cyber security, network performance, software-defined networking, and IT service design.

**Shi-Chun Tsai** received the B.S. and M.S. degrees from National Taiwan University, Taiwan, in 1984 and 1988, respectively, and the Ph.D. degree from the University of Chicago, USA, in 1996, all in computer science. He is currently a Professor in the Computer Science Department, National Chiao Tung University (NCTU), Taiwan. His research interests include computational complexity, algorithms, cryptography, Software Defined Networking and applications. Dr. Tsai is a member of ACM, SIAM and senior member of IEEE.

**Yi-Bing Lin** received his Bachelors degree from National Cheng Kung University, Taiwan, in 1983, and his Ph.D. from University of Washington, USA, in 1990. From 1990 to 1995 he was a Research Scientist with Bellcore. He then joined National Chiao Tung University (NCTU) in Taiwan, where he remains. In 2010, Lin became a lifetime Chair Professor of NCTU, and in 2011, the Vice President of NCTU. During 2014 - 2016, Lin was Deputy Minister, Ministry of Science and Technology, Taiwan. Since 2016, Lin has been appointed as Vice Chancellor, University System of Taiwan (for NCTU, NTHU, NCU, and NYM). Lin is an Adjunct Research Fellow, Institute of Information Science, Academia Sinica, Research Center for Information Technology Innovation, Academia Sinica, and a member of board of directors, Chunghwa Telecom. He serves on the editorial boards of IEEE Trans. on Vehicular Technology. He is General or Program Chair for prestigious conferences including ACM MobiCom 2002. He is Guest Editor for several journals including IEEE Transactions on Computers.

Lin is the co-author of the books Wireless and Mobile Network Architecture (Wiley, 2001), Wireless and Mobile All-IP Networks (John Wiley, 2005), and Charging for Mobile All-IP Telecommunications (Wiley, 2008). Lin received numerous research awards including 2005 NSC Distinguished Researcher, 2006 Academic Award of Ministry of Education, 2008 Award for Outstanding contributions in Science and Technology, Executive Yuen, 2011 National Chair Award, and TWAS Prize in Engineering Sciences, 2011 (the Academy of Sciences for the Developing World). He is AAAS Fellow, ACM Fellow, IEEE Fellow, and IET Fellow.