The Design of the Network Service Access Control System through Address Control in IPv6 Environments

Youngjoo Ahn[†] , *Seongjin Ahn* [††] *and Jinwook Chung,*[†]

[†] Dept. of Computer Engineering, Sungkyunkwan University
[††] Dept. of Computer Education, Sungkyunkwan University

Summary
This paper introduces a new design of a network service access control system using address control in IPv6 environments. In this system, We proposed network blocking and isolation method for unsured user or host.
The IPv6 network security management used should keep providing good performance to network devices and keep network load as low as possible as the network and the number of IPv6 nodes increases. To reduce this load, We do not use additional protocol stack and special network equipment. In this paper, a efficient method using IPv6 ICMPv6 is presented. We aim to minimize signaling and packet delivery cost while keeping access control service using address control.

Key words:
IPv6, Network security management, Network security, Access Control

Introduction

As the scale of modern day networks expanding, network administrators of firms, research institutes, and schools are spending more and more time and money on network address (IP/MAC) managements with no great efficiency. In addition, illegal network address usages by unauthorized personnel are causing network address collisions, network failures, and security issues.
The severity of such network management and security issues are not only presented in the current IPv4 networks, but also in the next generation IPv6 networks which are in occasion evaluated as some critical problems. This is because the same spoofing and sniffing attacks can technically be applied also on IPv6 systems.
Therefore, it is vital to develop a method that can significantly improve the reliability and stability of networks and systems through studies on real-time platform technologies that can secure network resources of network equipments and server terminals. This thesis plans on designing a system which can block and control networks to efficiently manage IPv6 network resources in real-time by monitoring the IP and MAC addresses used by a network in Link-Local units to execute network access control on unauthorized users and terminals and then isolating the terminal from the network. This can prevent a certain user from altering the IP address or the network interface card of network equipments or server terminals. In addition, the administrator can manage numerous network resources when introducing a new network resource equipment which allows efficient resource management and rapid response to network problems.

2. Network Service Access Control Methods

2.1 Network Access Control

This network access control system manages the network in Link-Local Scope units. It collects 2nd and 3rd level address situations through the agents installed per each Link-Local Scope unit and executes network access control based on related policies.

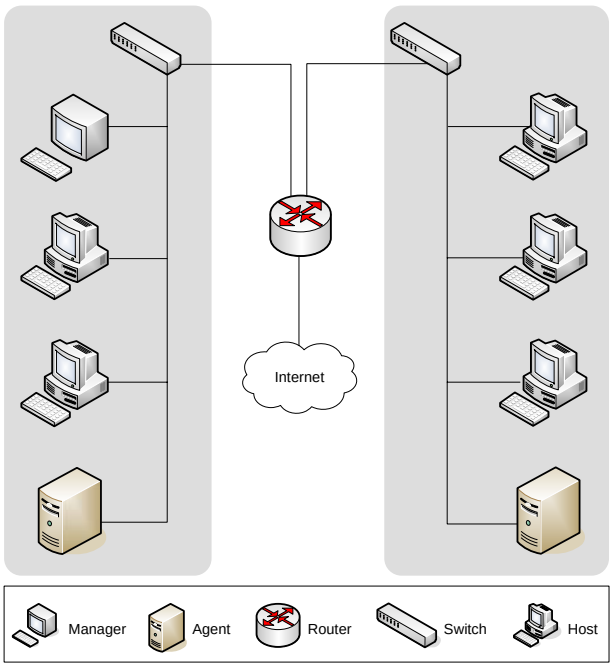

Fig. 1 Network Access Control System Model

* This work was supported by grant No. R01-2004-000-10618-0 from the basic Research Program of the Korea Science and Engineering Foundation.
** Dr.S.Ahn is the Corresponding Author.

The general host and agent making up a network each have one network interface card of which each card has one fixed interface ID. When a terminal in an IPv6 network receives a unicast address through automatic address creation and duplicate address detection processing the terminal will be granted access to the network. Therefore, it is necessary to acquire a method that manages address authentications to control network access.

The network access control of the IPv6 host is executed in procedures of collecting network resource information, blocking network entrance, isolation of the IP address in use from the network, and policy upkeep on continuous reuse attempts. Unauthorized users must reexamine their initial IP to use through an ICMPv6 message in order to access the network. The access control system here checks whether the user is authorized based on the policies stored per Link-Local Scope and sends an ICMPv6 response message in cases of when the user is unauthorized which eventually prevents that user from using the network address.

2.1.1 Network Resource Info Collection

To operate the access control system of a universal network resource, it is vital to be aware of the information on the available resources in the Link-Local Scope. With IPv4, a maximum of 254 ARP responses and endurable constant time of the request are required within the C-class unit network to search the IP resource in use. However, expansion of the host ID field length due to the expansion of the address length and available resource collection of sequential QA method due to automatic address allocation are actually impossible. To collect the available resources, monitoring period on the network information on initial system operation is required and this time is identical to the time out period of adjacent node access deny detection of the default gateway router.

There are two meanings when the information collecting period of network resources equals the time out period of adjacent node access deny detection. First, every IPv6 terminals existing in the Link-Local Scope within the time out period of adjacent node access deny detection must send at least one packet to the network. The IPv6 terminal keeps the IPv6 neighbor entry cache in its memory. The neighbor nodes registered in this neighbor entry cache refreshes the information in the neighbor entry cache when packets are received that sets the corresponding address as the sender. If packets that set the corresponding addresses as the sender are not received during the time out period of adjacent node access deny detection, the corresponding node is deleted from the neighbor entry cache. Second, the identical neighbor entry cache with other IPv6 terminals in the Link-Local Scope can be maintained.

2.1.2 Network Entrance Block

The host using an IPv6 address must go through a duplicate address search procedures. This process is undergone in cases of receiving IPv6 address resources through manual address creation or automatic address allocation or also in cases of receiving IPv6 address resources through automatic creation due to address allocation. Terminals that wish to receive an IPv6 address must use neighbor request messages in their own solicited-node multicast address through an ICMPv6 message and then request for a 2 layer address. When there is a 2 layer request on the unauthorized host, the access control system creates and sends a response through a neighbor notification message to hide the fact that the corresponding IP resource is in use. If a duplicate address is found, the corresponding address cannot be allocated to the network interface.

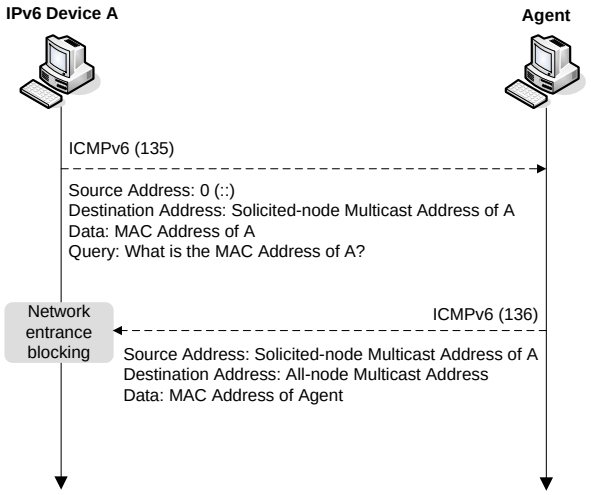

Fig. 2 Network entrance blocking feature of an agent

2.1.3 IP Resource Isolation

Isolation of the IP resource in current use from the network requires methods other than binding it with the network interface through duplicate addresses. A method to handle neighbor request messages and path redirection messages is used in such cases.

The method to handle neighbor request messages is used to prevent authorized hosts from sending packets to hosts to isolate. Firstly, set the IPv6 address to isolate from the network as a 3 layer sender address and then create a neighbor request message with an address of other terminals located in the Link-Local Scope like the isolation subject terminal B. The data in this packet holds random 2 layer addresses and such packets are sent to the

network. External terminals located within the Link-Local Scope alike the terminals subject for isolation has 2 layer addresses that holds data of packets that are created and sent by the agent at their neighbor entry cache and therefore these two random 2 layer addresses are used to send packets through the IP resource subject for isolation. In this case, the 2 layer address subject for address change request does not exist in the actual network or is the 2 layer address of the agent which prevents all terminals within the network affiliated to terminal B that is subject for isolation from sending packets to terminal B.

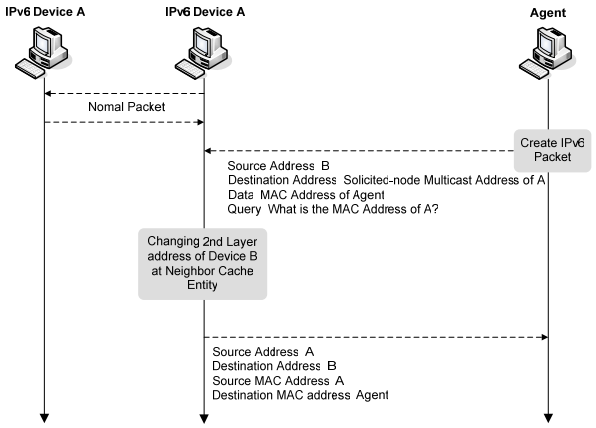

Fig. 3 Network isolation through address change

The handling method of path redirection messages is used to make the host targeted for isolation to misrecognize the next hop for packet transfer. This prevents the IPv6 terminal subjected for isolation from sending packets within the network by targeting the IP resource for isolation and setting the wrong data for the next hop address.

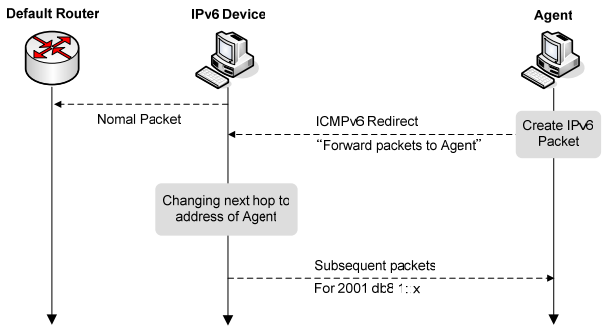

Fig. 4 Network isolation through redirection messaging

3. Network Service Access Control System

3.1 System Outline

The network service access control system can be distinguished into two features. Its first feature provides network resource information to the administrator and executes control functions. Its second feature directly controls the network resources through monitoring data and manual configurations of the administrator. For a proper designing of such features, it is required to distinguish the network resource monitoring program for resource collection notice and administrator function input with network access control agents that are in charge of Sniffing and Snoofing of IPv6 neighbor search protocols. This thesis gives a detailed description on the design and operation of the network access control agent but not on the detailed design of the network resource monitoring program.

Table 1: Features of the network service access control system

Management	Control
Automatically collects network addresses	Secures authenticated network addresses
Collects network terminal information	Blocks unauthorized network addresses
Notifies of any IP collisions	Isolates the network of an aggressive user
Collects error data	

3.2 Application of Network Service Access Control

The management system provides a feature to monitor IP addresses which is used in the current network. By using this system, the administrator can check IP address usage in real-time and block the IP addresses of unauthorized users based on the collected IP and MAD address resource information form the agent system.

3.2.1 Application of Network Info Collecting

The agent monitors all neighbor search protocols that are sent and received within the Link-Local Scope and independently records it in the DB system. The DB system receives network and IP information collected by the dispersed agents. Such information is centrally managed to prevent duplicate IP address usage and gather statistics on the overall IP usage.

During system activation and time out period of initial adjective node access deny detection, It is required to monitor not only the neighbor search protocols but also all IP packets that are collectable within the Link-Local

Scope. Collection of neighbor search protocols and detection of network connection on packet forwarding which starts during the initial network information collecting period after the first system activation is possible. It is because the IP address is converted into 2 layer MAC address when initially sending a packet. However, the sending and receiving of neighbor search protocols may not be found in cases of network connection valid before the system became active because the 3 layer IP address and 2 layer MAC address are all stored in the neighbor entry cache. But such monitoring on all IP packets are only required during the initial operation. After packet monitoring during the time out period of adjacent node access deny detection, monitoring the neighbor search protocol alone can maintain an updated network resource.

3.2.2 Application of Network Access Control

The administrator blocks the IP address of unauthorized users and the ones that violates the related policies to block access to the network service and strengthen its security.
Fig. 5 describes the process that blocks access to the network service by preventing a specific IP address from binding with the network interface in a situation where the administrator orders a blocking command on a specific IP address with a monitoring program. In a IPv6 system, its host ID is almost impossible to post unlike the IPv4, so a method that issue options that allows the IP resource to be usable in the monitoring program must be applied. In the case where the IPv6 terminal tries to access the network service, a normal network address binding is authorized if the IP is authorized but otherwise it must be prevented.

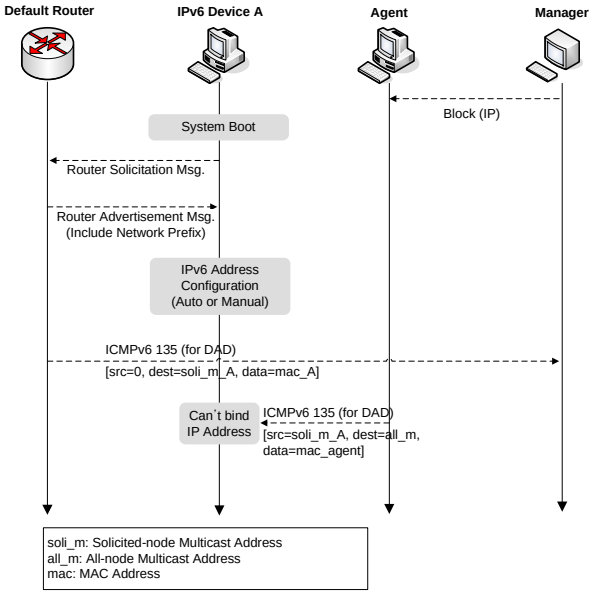

Fig. 5 Block process of unauthorized IP addresses

Even the network access control method of allowing network address resources to only the authorized users cannot completely prevent an illegal use of the network address resources with an IP address disguised to be of the authorized major network equipments and server resources. Such problems can be solved using a method that fixes the IP address through the binding of IP and MAC addresses. In the case where attempt is made through a MAC address fixed to the corresponding IP through the monitoring of the packet that is starting the duplicate address inspection for network address acquirement, no interruption in network address acquirement through packet creation is made and response is made to duplicate address requests in alternate cases which prevents the network address resource with a fixed IP from binding with network interface cards with MAC addresses other the ones set by the administrator.

3.2.3 Application of Network Isolation

The administrator can check the addresses of the currently available network resources through a monitoring program and isolates the network address resource of an unauthorized user from the network to block network access services. If data of the name allocated in the IPv6 terminal, OS type, or other software and hardware information can be simultaneously collected and stored in a separate database during the network information collecting process, the administrator can issue a more accurate judgment on whether the IP address is owned by an authorized user or an unauthorized user.
Fig. 6 describes the process that isolates the terminal that is deemed to be used by an unauthorized user from the network. In the situation where IPv6 terminal A receives a network prefix from a default router in the network to perform a normal IP address binding, the administrator orders a network isolation command through a monitoring program. The agent creates and sends a packet to IPv6 terminals B and C which disguises the agent of owning the 2 layer MAC address of IPv6 terminal A, and then updates the Neighbor Entry Cache of terminals B and C. It also notifies terminal A the agent address as the default router address to allow the IPv6 terminals A, B, C to send packets to the agent and isolate the IPv6 terminal A from the Link-Local area.

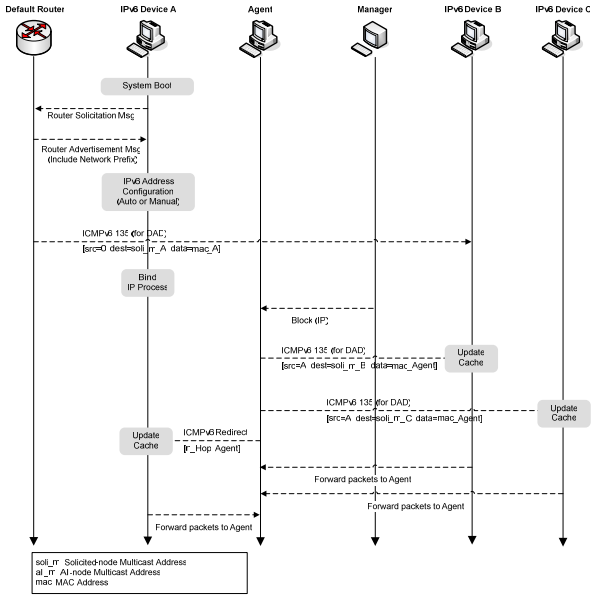

Fig. 6 Network isolation process of an IP address

Conclusion

Based on the IPv6 network, this thesis designed a system which prevents unauthorized users from using the network through the features such as network address setup, duplicate address exploring, layer address change, and path redirection that are controlled by ICMP and ARP of an IPv4 system that allows an IPv6 terminal to access the network and receive IPv6 resources or from preventing unauthorized users from continuous use of the network server through pre-assigned resources.

The network service access control system on IPv6 address control requires a more complex form of features than the ones in IPv4 due to enhancements in security and IPv6 address application and also consumes more system and network resources. However, the network service access control system presented in this thesis can be also employed only through agents in Link-Local Scope units according to security policies and the presence of security-threatening users without additional protocols or the employment of special network equipments for management.

However, there is the problem where of load generating due to packet creation on all terminals within a Link-Local system or terminals other than the ones subject for blocking. Such performance-related problems due to the absence of packet transfer methods in broadcast formats are deemed to improve in future researches.

References

[1] Kang Hong Cho, Seongjin Ahn, Jin Wook Chung, "Rule-based Agent system for Fault Detection and Location on LAN", KIPS, vol. 7-7 pp.2169-2178, 2000

[2] Forouzan, “TCP/IP Protocol Suite 2nd Edition”, 1997

[3] Taein Hwang, Seongjin Ahn, Jin Wook Chung, “A study on the rules and algorithm for the diagnosis and recovery of routing configuration” , WMSCI 2000, World Multiconference on Systemics, Cybernetics and Informatics 4 137-141, 2000

[4] T. Sugawara, “ Acooperative LAN diagnosistic and observation expert system, computers and communications”, Proceeding of the Ninth Annual International Phoenix Conference, pp. 667-674, 1990

[5] J.-M. Yun,, S.-J. Ahn, J.-W. Chung, “Web Server Fault Diagnosis and Recovery Mechanism Using INBANCA”, PP. 2467-2504, 2000

[6] Yunseok jang, Seongjin Ahn, Jin Wook Chung, “RBR Based network Fault Detection and Recovery System using Agent Collaboration”, ICOIN, 2003

[7] Kato, K., “Persistently Cashed B-trees”, IEEE Transactions on, Volume: 15, Issue: 3, Pages 706-720, May-June 2003

[8] H. Weatherspoon, T. Moscovitz, J. Kubiatowicz, “Introspective Failure Analysis: voiding Correlated Failures in Peer-to-Peer Systems”, Proceedings of International Workshop on Reliable Peer-to-Peer Distributed Systems, Oct 2002

[9] Kyohyeok Kwon, Seongjin Ahn and Jinwook Chung, “Network security manage-ment using ARP spoofing”, Proceedings of ICCSA 2004, 2004

Youngjoo Ahn received the B.S. degree in computer education from Sungkyunkwan University, Korea in 2005. She is currently working towards the M.S. degree in computer engineering with the School of Computer Engineering, Sungkyunkwan University, Korea.

Seongjin Ahn received the B.S., M.S. and Ph.D. degree in information and communication engineering from Sungkyunkwan University, Korea in 1988, 1990 and 1998, respectively. For more than five years, he was a Researcher in Electronics and Telecommunications Research institute (ETRI), Korea. He is currently an assistant professor department

of computer education, Sungkyunkwan University, Korea. His research interests include network management, network security, and information assurance.

Jinwook Chung received the B.S. and M.S. degree in electric engineering from Sungkyunkwan University, Korea in 1974, 1977, respectively, and the Ph.D. degree in computer science from Seoul National University, Korea, in 1991. For more then ten years, he was a section chief in Electronics and Telecommunications Research institute (ETRI), Korea, since 1984 he has been a professor of the school of Information and Communication Engineering, Sungkyunkwan University, Korea. In 2002 he served as President of the Korea Information Processing Society (KIPS). His research interests include data communications, computer networks, network management, and network security. He has guided more than 150 M.S./Ph.D. students in this area of study and has published more than 100 papers in technical journals and conference proceedings.