[Work in Progress] 研究報告

Modification of IP Address Management Database with Network Access Authentication

Kazuyuki Miyakita[1,a)] Kazuyuki Yamamoto[1] Shigeyoshi Aoyama[1] Kenji Mikawa[1]

Niigata University introduced an network access authentication based on MAC addresses in March 2009. In addition, we developed an IP address management database (IPDB), which registers and manages information related to each global IP address, to enhance information security and to reduce the load on department administrators. IPDB operates simultaneously with the network access authentication system, and an authentication for a devise is realized by automatically writing an access list to an L2 switch by using the information registered in IPDB.

In [1], we proposed an extension of IPDB to visualize the registered information for management improvement. For further improvement of management, in this report, we modify IPDB such that the registered information that has not been used (i.e., has not been authenticated) for a long time is automatically deleted. Here, we set the threshold elapsed time to 5 months.

The following are the specific operations of the modified part of IPDB.

- We make a table consisting of IP addresses for devices that do not need an authentication (e.g., devices of the core network system) on the database in the IPDB server in advance. The table is denoted by *cais_ip*. *cais_ip* is used to avoid deleting the IP addresses for such devices.
- A log server in the network access authentication system periodically transfers the list of IP addresses that were successfully authenticated in the previous day to the IPDB server once a day at early morning. This operation is realized by automatically executing a script file deployed on the log server.
- The IPDB server makes (or updates) a table consisting of a pair of an IP address and the last authenticated date for the IP address on its own database. The table is denoted by *access_date*. Specifically, the IPDB server refers each IP address in the list received from the log server, and
  - replaces the value of date for the corresponding record in *access_date* with the previous day if *access_date* includes the IP address,
  - adds a new record consisting of a pair of the IP address and the previous day to *access_date* otherwise.

  This operation is realized by automatically executing a script file deployed on the IPDB server.
- Based on *cais_ip* and *access_date*, the IPDB server deletes the registered information that has not been authenticated for 5 months from IPDB. Specifically, the IPDB server compares each record of IPDB with the two tables in the following order.

  (1) If the IP address corresponding to the record of IPDB exists in *cais_ip*, then the IPDB server does not delete the record from IPDB.

  (2) If the IP address corresponding to the record of IPDB exists in *access_date*, and the last authenticated date for the IP address is later than 5 months from today, then the IPDB server does not delete the record from IPDB.

  (3) Otherwise, the IPDB server deletes the record from IPDB.

  This operation is also realized by automatically executing a script file deployed on the IPDB server.

In the presentation, we show some test results and discuss the effectiveness of the proposed modification.

References

[1] K. Miyakita, K. Yamamoto, S. Aoyama, and K. Mikawa, "Operation and Extension of IP Address Management Database with Network Access Authentication," IPSJ SIG Technical Report, Vol. 2016-IOT-33, No. 2, pp. 1–6 (2016).

[1] Center for Academic Information Service, Niigata University, Japan
[a)] miyakita@cais.niigata-u.ac.jp