Virtual Private Network Authentication System Featuring High Extensibility and Availability: AAA

Kenichi Matsui†, *Kenji Ota, Hiroyuki Kurita, Hitoshi Nagao, Kenichi Mase, and Shinya Matsumoto*

Abstract

NTT Network Service Systems Laboratories has developed an authentication system, called AAA, that authenticates users when they try to access a virtual private network (VPN). It features both high extensibility, which is the ability to flexibly combine multiple authentication methods depending on how a given user uses a VPN service, and high availability, which is the ability to avoid service disruption even in the event of a serious disaster.

1. Introduction

As the computerization of office operations advances, it has become common to interconnect local area networks in multiple office sites to carry out office operations in an integrated manner. This interconnection is increasingly being done using virtual private network (VPN) services, which are cheaper than leased-line services. In Japan, the use of VPNs now surpasses that of leased lines, especially in the case of enterprise users: about half of all enterprise users now opt for VPNs [1].

Unlike leased lines, VPNs are configured on a public network, which can be accessed by the general public. Therefore, an authentication system is needed to ascertain that someone trying to access a VPN has the authority to do so.

A VPN authentication system must provide three basic functions: an authentication function to identify the user correctly, an authorization function to check whether the user has the authority to use the requested service according to the contract with the user, and an accounting function to record the user's usage. These three functions are collectively known as AAA. A VPN authentication system equipped with these functions can authenticate users, determine whether or not the user should be permitted to access a given service, and manage usage records for all users.

Although VPN authentication systems normally use only a user ID (identification) and password for authentication and authorization, rising concerns about security are leading to demands for the use of multiple authentication factors, such as identification of the user's access line, in addition to user ID and password [2]. VPN authentication systems are required to be able to provide different combinations of authentication and authorization flexibly depending on the needs of each service.

As VPN services become widely utilized, an increasing number of enterprises are applying VPNs to systems that require high availability, such as their core business systems, but a failure in such systems could cause considerable damage. Therefore, VPN authentication systems need to provide high availability to avoid service disruption even in the event of

† NTT Network Service Systems Laboratories
Musashino-shi, 180-8585 Japan

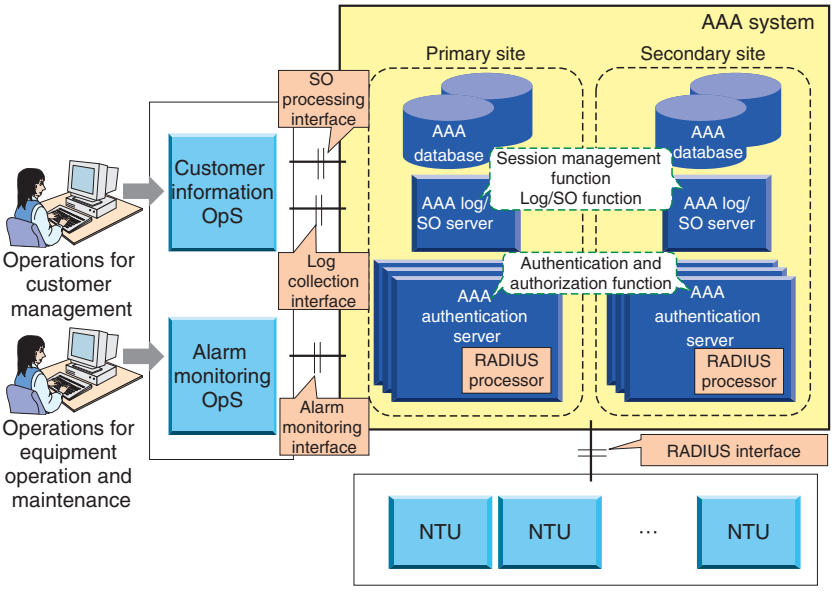


Fig. 1. Overall configuration of AAA.

a serious disaster.

To meet these requirements, we have developed a VPN authentication system, called AAA, that has high extensibility and availability in processing authentication and authorization. This article describes the configuration, functions, and features of this system, which has already been implemented.

2. System configurations and functions

2.1 Configuration

The overall configuration of our system is shown in **Fig. 1**. The AAA consists of three parts. The AAA authentication server performs authentication and authorization. The AAA log/SO server collects and formats logs, processes service orders (SOs), which are users' service provisioning requests, in collaboration with the operations system (OpS), and manages session information. The AAA database stores information about authentication derived from service orders, information about equipment, and information about established sessions.

In preparation for serious disasters, the AAA is duplicated at two sites. The number of AAA authentication servers can vary depending on the number of connected network termination units (NTUs), which control user terminals.

2.2 Authentication and authorization functions

The AAA exchanges authentication information with NTUs using RADIUS (Remote Authentication Dial-In User Service), which is a user authentication security protocol. The basic operation of the system up to the establishment of a VPN connection is as follows (**Fig. 2**):

(1) The router or home gateway in the user network sends the user ID and password to the NTU to request a VPN connection.

(2) The NTU requests the AAA to authenticate the user using the network information (e.g., line identification) that it possesses, in addition to the user ID and password.

(3) The AAA determines whether the connection should be permitted by referring to the authentication and authorization request from the network terminal unit and the user's authorization conditions stored in the database. It sends its decision back to the NTU.

(4) The NTU either starts or rejects the requested VPN connection depending upon the reply from the AAA. If a connection is to be started, the NTU asks the AAA to start recording the session for accounting. The AAA records the session information, which shows the state of the user's connection (access line identification, connection start time, IP address given, etc. (IP: Internet protocol)).

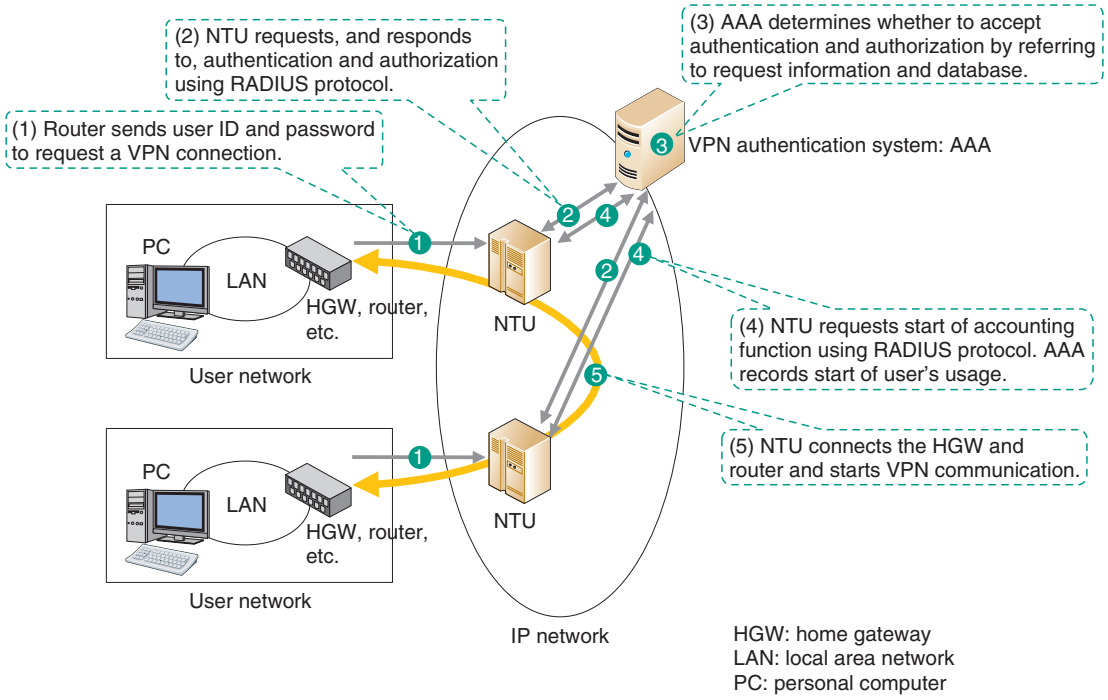


Fig. 2. Basic authentication operation up to VPN connection establishment.

(5) The NTU connects the user terminal, and VPN communication is started.

In this way, the AAA authenticates and authorizes VPN users in a highly secure manner on the basis of the user ID, password, and line identification (in this example).

2.3 VPN session management function

The AAA holds the session information about the user who has been connected to the VPN after authentication has been completed. This session information is used to prevent double logins from the same user and is also referred to when maintenance staff check the connection state to deal with a complaint from the user.

As the user's connection state changes (connection establishment or release), the session information held by the AAA is updated on the basis of information contained in RADIUS messages sent by the NTU. If the RADIUS messages fail to reach the AAA owing to packet loss or a fault in the NTU, the session information held by the AAA may become different from the user's actual connection state. To resolve such a discrepancy, the AAA collects the user's connection information from the NTU and automatically corrects the session information concerned. Specifically, this function operates as follows (**Fig. 3**):

(1) The AAA log/SO server obtains the session information list from the AAA database.
(2) It obtains the session information list from the NTU.
(3) It compares the two lists: if they do not match, it replaces the session information in the AAA database by that held by the NTU.

This session information correction can be executed without suspending the operation of the AAA and enhances the reliability of the session information. Session information can also be sent to devices other than the AAA for use in authentication by upper-layer applications, such as ASP (application service provider) services and SaaS (software as a service).

2.4 SO function

The SO function updates the SO information needed for VPN authentication in collaboration with the OpS. It registers, updates, deletes, or refers to SO information in the AAA database in response to an SO request sent by the OpS. In addition, it asks the NTU to release the user's session.

The SO function and the OpS exchange messages written in XML (extensible markup language) using

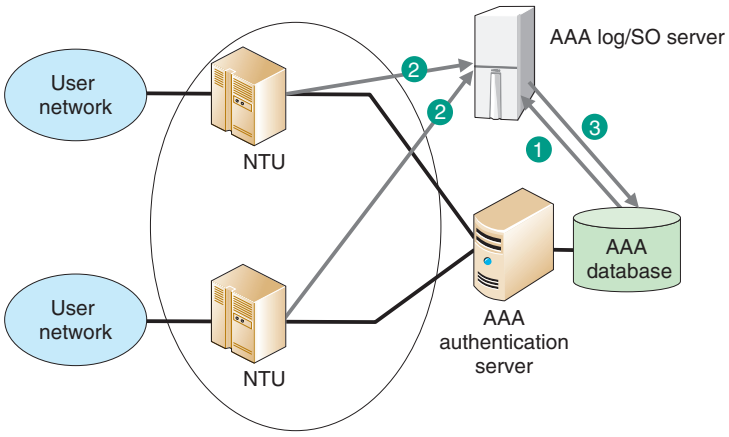


Fig. 3. Operation of session information correction.

the message exchange protocol SOAP (simple object access protocol) to ensure versatility and extensibility in authentication.

3. Features

3.1 Provision of usage history reports

The AAA can provide the history of each user's authentication and authorization in the form of a report.

The VPN authentication server normally outputs the information included in RADIUS messages sent from NTUs, to the authentication and authorization log. However, in a VPN service, which can be accessed from lines of various types, the NTUs used may also vary. Attributes included in RADIUS messages can vary depending on the type of NTU. Therefore, it is not straightforward to generate a usage history report from authentication and authorization logs.

To solve this problem, items that are output in usage history reports (events, such as the start and end of usage, date and time when each event occurred, user ID, line number, etc.) are defined for each type of NTU.

3.2 Extensibility of authentication and authorization function

The number of items that the authentication and authorization function must check is growing. To be able to cope with such an increase flexibly through the simple addition of necessary functions, the AAA has extended interfaces (**Fig. 4**).

The extended processing part obtains or changes information needed in the processing of authentication and authorization, such as user ID, password, and network information, through an extended interface. When a new authentication and authorization module is added, the module obtains the necessary information and returns processing results to the basic processing part through the extended interface so that the processing results will be reflected in the authentication and authorization. Since extended functions can be added without modification of the AAA's basic processing part, new authentication and authorization capabilities can be easily added to meet new user needs.

An extended interface is available for each of the three stages of processing: processing concerning all users, processing concerning only legitimate users, and processing concerning authorization. This arrangement makes it possible to select an extended interface appropriate for a specific processing operation or to select an appropriate method of adding functions in order to achieve high-speed processing. For example, processes executed for only legitimate users, such as authentication and authorization processes, for which the occurrence number is proportional to the number of user sessions, can be applied after the authentication of individual users. This will limit the number of users handled by these processes and thus eliminate wasteful processing.

3.3 Compatibility of availability and high-speed processing

In preparation for major disasters, the AAA has a redundancy configuration in which a system is installed at each of two sites: the primary site and the

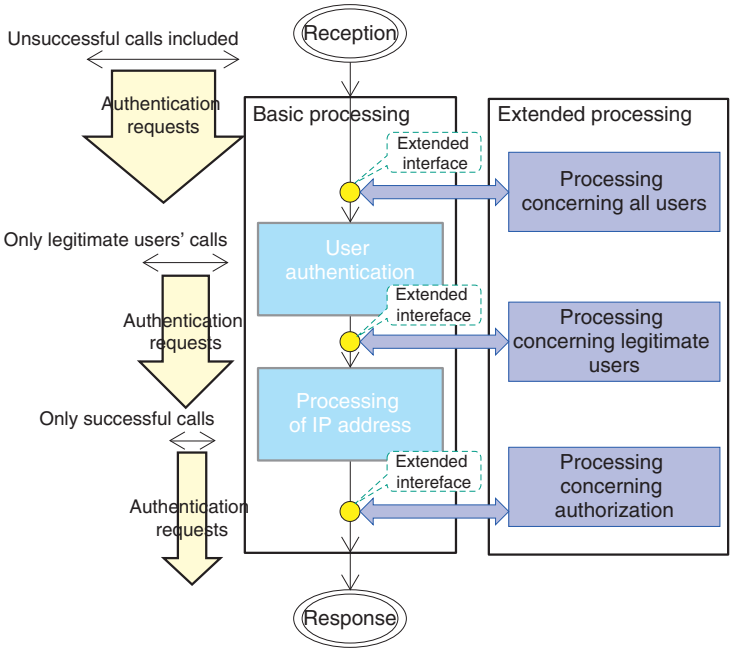


Fig. 4. Extensibility of the authentication/authorization process.

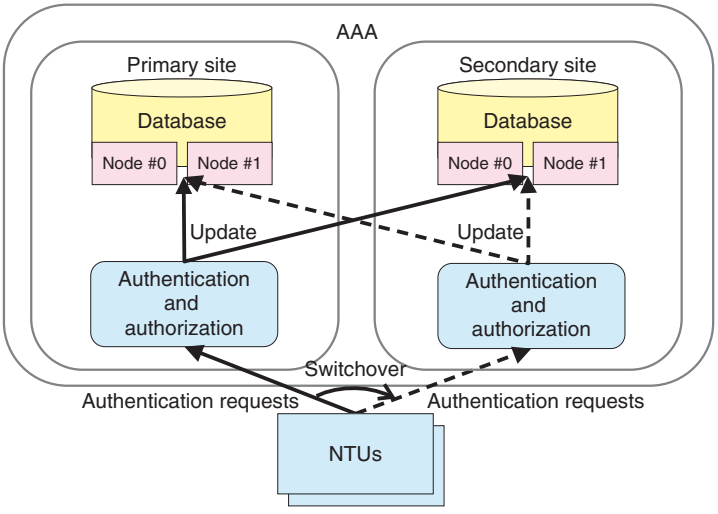


Fig. 5. Redundancy configuration of the AAA system.

secondary site (**Fig. 5**). Both systems are kept active. If the system at the primary site is disrupted, all NTUs switch over to the system at the secondary site, which continues to provide authentication and authorization.

To support the switchover to the secondary-site system, the databases at the two sites must be synchronized in real time to ensure consistency in the checking of double logins and other processing. To meet this requirement, database updating is executed at the two sites simultaneously so that the contents of the two databases are always synchronized. To enhance the authentication response performance, access to the databases is minimized. For example,

the system that has received a request for authentication refers only to its own database, and it sends an authentication reply to the requesting NTU only after it has successfully updated its database. The other database will be updated after the authentication reply has been sent. This arrangement makes it possible to keep duplicate data for authentication and authorization at two sites while ensuring high-speed authentication. For even higher availability, each site has a cluster of two data servers.

4. Conclusion

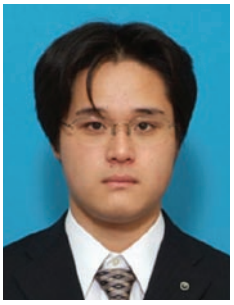
The AAA authenticates users when they try to access a VPN. It features both high extensibility and high availability. It is currently used in the FLET'S VPN Wide Service (offered by NTT EAST since August 2010 and by NTT WEST since November 2009). Building upon the core authentication technology developed through these research and development activities, we will study technologies that enable users to access a variety of network services on VPNs, such as ASP and cloud services, safely, securely, and conveniently.

References

[1] Nikkei BP, "Fact-finding Survey of Networks 2010," NIKKEI NETWORK, No. 123, pp. 046–047, July 2010 (in Japanese).
[2] B. Nagel, "Password Seeks Partner for Long-term, Secure Relationship," CIO, Vol. 11, No. 2, pp. 28–31, 2010.

Kenichi Matsui
Senior Research Engineer, Third Promotion Project, NTT Network Service Systems Laboratories.
He received the B.E. degree in information engineering and the M.S. degree in information sciences from Tohoku University, Miyagi, in 1995 and 1997, respectively. He joined NTT in 1997 and studied IP networking technology including IP multicast management, quality-of-service management, and traffic engineering. During 2005–2008, he was engaged in commercial development of IPTV and video-on-demand services. He is currently focusing on R&D of the Next Generation Network. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), and IEEE.

Kenji Ota
Research Engineer, Third Promotion Project, NTT Network Service Systems Laboratories.
He received the B.S. and M.S. degrees in mathematics from Keio University, Kanagawa, in 1989 and 1991, respectively. In 1991, he joined NTT Software Laboratories, where he engaged in R&D related to requirement engineering. He has been engaged in R&D concerning software engineering, IPv6 network operations, and secure network access. During 2001–2004, he was engaged in developing commercial services for the Global IP-VPN. His work is currently focused on R&D of the Next Generation Network. He is a member of IPSJ.



Hiroyuki Kurita
Engineer, Third Promotion Project, NTT Network Service Systems Laboratories.
He received the B.E. and M.E. degrees in information and communication engineering from the University of Tokyo in 2005 and 2007, respectively. He joined NTT Information Sharing Platform Laboratories in 2007 and studied network security including authentication and network attachment control. His work is currently focused on R&D of the Next Generation Network. He is a member of IEICE.

Hitoshi Nagao
Senior Research Engineer, Third Promotion Project, NTT Network Service Systems Laboratories.
He received the B.E. degree in information engineering from Tokushima University in 1993. He joined NTT in 1993. He is currently focusing on R&D of the Next Generation Network.

Kenichi Mase
Research Engineer, Third Promotion Project, NTT Network Service Systems Laboratories.
He received the B.E. degree in electrical engineering from Toyo University, Tokyo, in 1991. He joined NTT in 1991. He is currently focusing on R&D of the Next Generation Network.

Shinya Matsumoto
Research Engineer, Third Promotion Project, NTT Network Service Systems Laboratories.
He received the B.E. and M.E. degrees in electronics and electrical engineering from Doshisha University, Kyoto, in 1987 and 1989, respectively. He joined NTT Communication Switching Laboratories in 1989 and studied intelligent networks. His work is currently focused on R&D of the Next Generation Network.