Broadband Service Gateway Platform for Readily Available and Reliable Business Applications and Services

By Motoo NISHIHARA,* Satoshi KAMIYA,* Takeo HAYASHI,* Hiroshi UENO,† Tomoyasu DOMEKI† and Toshiyuki KANOH*

ABSTRACT The progress of broadband Internet has caused various changes in services such as shopping, banking, and entertainment. Today, many customers can use various high-quality services over broadband Internet anytime and anywhere. As the services utilizing broadband Internet come into wider use, the availability and the reliability of the services become important subjects. This paper introduces a broadband service gateway platform technology that makes various businesses and services over the Internet readily available and reliable. A concept of a network front-end processor at the boundary between an information system and the network is proposed.

KEYWORDS **Broadband Internet, Integrated IT and NW system, Hardware acceleration engine**

1. INTRODUCTION

The service industry has changed with the advent of widespread access to broadband Internet. Personal computers and all the information systems in enterprises, in the home, and in those belonging to individuals are now connected by broadband Internet. Also, through the high-speed network, anyone is able to take part in good quality business endeavors, and use various services anytime, anywhere. Advertising media has changed from newspapers or handbills to pop-up windows, while ticketing counters and shops have been replaced by WWW pages.

If there is a high dependence on broadband Internet and the information systems of enterprises, individuals, or the community, it seems likely that broadband Internet and information systems will become utilities similar to electricity, gas, and the telephone line. In such conditions good quality, good stability, and reliability of broadband Internet and information systems become important issues.

However, because everyone is able to access information systems through the high-speed network, the load on information systems will become very large. This is unavoidable. Significant problems that need to be overcome include reducing the load on information systems and protecting the systems from the cyber-attacks by malicious users.

This paper proposes a network front end function that mitigates the load of an information system and protects the information system itself from cyber-attack. A broadband service gateway platform is introduced. The platform can execute the network front end function at a rate of gigabits, at the boundary between an information system and the network.

2. MAINTAINING THE QUALITY AND PERFORMANCE OF A BUSINESS AND OF SERVICES

2.1 Problems with Widespread Access to Broadband Internet

With widespread use of broadband Internet, all businesses and services now have a high dependence on information systems and the broadband Internet. In particular, general access to broadband Internet not only improves the capability to access information systems, but also allows more users to have access to the systems.

Overloading of an information system by a large number of accesses can result in the system going down, and causes the business or service to discontinue operations. Although computer and semiconductor technology is evolving remarkably quickly and also improving the performance of server systems, the increase in the number of accesses and the daily demand for performance improvement outweighs any improvement.

Also, because many and unspecified accesses are be permitted, the problem of intrusion and users altering information with malicious intent are becoming more of a concern.

*System Platforms Research Laboratories
†Ubiquitous Platform Development Division

2.2 Countermeasures to Increase in the Quality of Business Services

Some methods to avoid the bottleneck of an information system, caused by cyber-attack and the increased load of information systems, have already been employed.

A typical way of reducing the load placed on an information system is called "Load Distribution (Load Balancing)." This method uses two or more server systems to carry the same application software and distributes a load between them. However, this method has the drawback that two or more server systems with application software are needed, which increases the investment cost and the management cost (**Fig. 1**).

Another way to reduce the load is called "Off-Loading." Part or all of the functions that have a heavy load are separated from the server system. These dedicated systems reduce the load imposed on the server system (**Fig. 2**).

Currently, firewall or encryption functions are off-loaded from the server system and are arranged as a dedicated system (security appliance). However, the dedicated system only has a single function, and information systems usually need several different dedicated systems. This results in system complication or an increase in the system cost (**Fig. 3**).

3. PROPOSED BROADBAND SERVICE GATEWAY

3.1 Network Front End Function

In order to protect businesses and services from the various bottlenecks and to obtain a good business and service environment, the load distribution and the off-load methods have already been realized and used.

To enhance these methods and develop new techniques, the functional deployment of an information system and a network system has been rearranged. It is our belief that the integrated IT&NW system needs to be optimized further.

In order to attain good performance, reliability, stability and safety of an information system, some functionality is separated from the server system and implemented as a unified, dedicated system. In general the function is called a "network front end function." The functions of the network front end include:

1) System security functions, such as intrusion detection/protection, an anti-virus function, and a firewall function.
2) Functions that prevent information leaks, such as encryption and monitoring.
3) Network functions, such as traffic distribution and control.
4) Access-control function represented by the VPN, such as user certification and proxy systems.

By integrating the functions, which are currently realized individually, into a dedicated system that has good performance and cooperation between functions, it is possible to optimize the flexible integration of IT & NW systems.

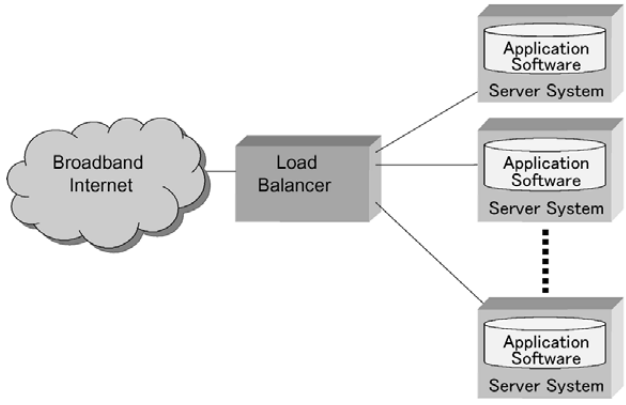

Fig. 1 Load balancing.

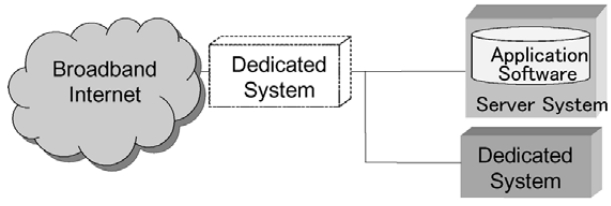

Fig. 2 Off-loading.

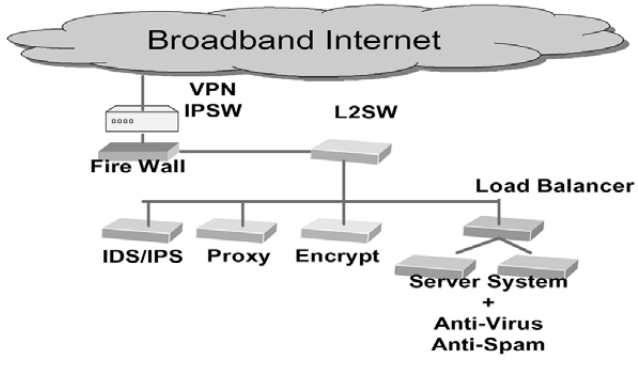

Fig. 3 Configuration of information system.

3.2 IT & NW Integrated System Architecture

Figure 4 shows an example of the proposed IT&NW integration-system architecture.

By improving the performance of the individual functions of an information system and integrating these functions into a network front end function at the boundary between an information system and broadband Internet, it is possible to realize a business and service environment that is reliable, stable and of good quality.

3.3 Function and Performance Requirements at the Network Front End

Although the network front end functions are detailed above, because functionality needs to corresponds to the business model and the service model (which is evolving day by day), the network front end function should also evolve. The functions of the network front end include the following basic functions.

1) The function to perform packet recognition and termination on the TCP/IP level.
2) The function to identify a session and traffic on the application or contents level.
3) The function to perform session and traffic control (bandwidth, distribution), based on a recognition and identification result.
4) The function to perform a part of the application (protocol) processing function.

The network front end function is a combination of the above basic functions.

Moreover, since the network front end function is arranged on the boundary between a network and an information system, it should be able to cope with the maximum network traffic throughput. Also, the performance should be realizable at a sufficiently low cost as compared with the cost of using conventional methods.

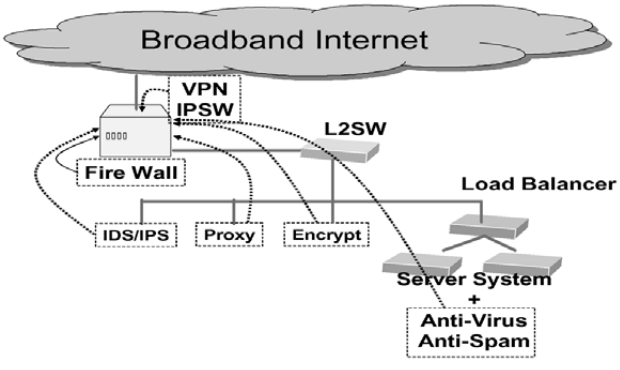

Fig. 4 IT&NW integrated system architecture.

To achieve this, the hardware and software of the processing function has been changed. Several hardware engines that execute most of the network front end functions have been developed.

3.4 Hardware Engine for Good Performance and Stability of the Network Front End Function

An efficient way to improve the performance of a software function is to use a hardware engine. If a new algorithm and architecture is suitable, hardware can be devised. Performance improvement of several orders of magnitude can be achieved.

On the other hand, the advantages of software include the flexibility to add functionality, and the simplicity of being able to use a functional description. Therefore, in general, in order to build a highly efficient system, the software (the network front end basic function) is transformed into a hardware engine. It is also effective for the hardware engines to share the processing function of an application module with the software. However, it is usually dependent on the function that the operating system possesses.

The layer structure of the functions within the network front end function is shown in **Fig. 5**. The TCP/IP off-load engine LSI and expansion board are commercialized with emphasis on improving the performance of the network front end function.

However, the role of the LSI and the board (hardware engine) is only a part of the function and the performance still depends on the performance of the operating system's software. For example, the conventional hardware TCP engine only executes a data transfer function, and most of the protocol controller and the data reconstruction function are dependent on the performance of the operating system's software. As the result, it cannot cope with the establishment of a lot of TCP sessions because of a bottleneck

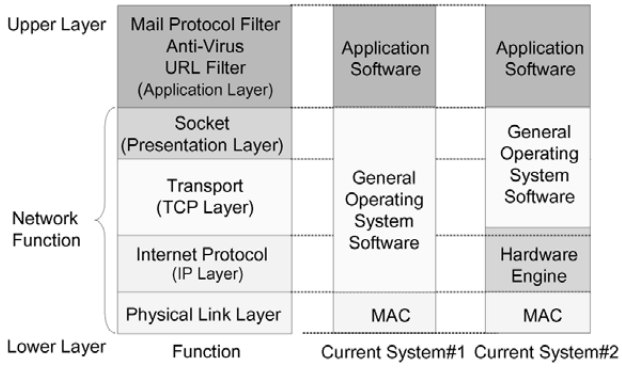

Fig. 5 Conventional functional class structure in an information system.

in the performance of the operating system's software. The session establishment performance in the current system is several 100 connections/second.

However, the broadband service gateway which integrates and connects several network front end functions into a single system, needs the processing performance to be several gigabits, which is 10-100 times higher than that of the conventional system. The broadband service gateway is required to improve on the conventional concept of hardware and software functional load dispensation, and to build a new system platform.

The functional distribution within the platform, which is appropriate for the example of e-mail transfer, is shown in **Fig. 6**.

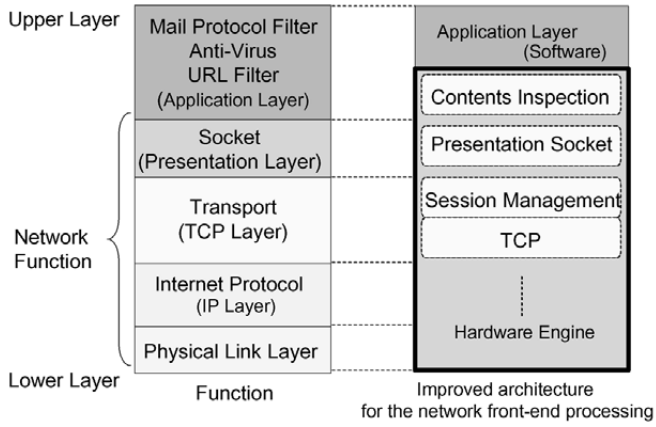

Fig. 6 Improved architecture for high performance and high stability.

4. REALIZATION OF A HARDWARE ENGINE WHICH STRENGTHENS THE BROADBAND SERVICE GATEWAY

4.1 TCP, Socket and Presentation Hardware Engine

We have developed a hardware engine for the TCP, socket, and presentation functions in an operating system. The performance is 1,000 times better than for the conventional system.

As a result, the session establishment performance of the new TCP hardware engine was 160,000 sessions/sec., which is 1,000 times better than the rate of the BSD4.4 Lite operating system software. Moreover, the socket and presentation engines achieved a performance rate as good as the TCP engine. This was achieved by improving the algorithm and original architecture. The composition and performance of the hardware engine are shown in **Fig. 7** and **Table I**.

4.2 Contents Inspection Hardware Engine

A contents inspection hardware engine has been developed. It identifies the contents that flow through a network (e.g. the body and subject of e-mails, command of an application, and script), and allows both high speed operation and flexibility (programmability). This engine consists of the Field Extract section, which extracts the keyword from the data, and the Table Search section. The Table Search section searches at high speed for the relative information, which is located in a database, about the keyword. A block diagram of this engine is shown in **Fig. 8**.

This engine enables the extraction of any keyword from a packet data stream and checks for the keywords within the database to find the contents level at a rate of one million times per second. For example, by using this engine for the E-mail contents

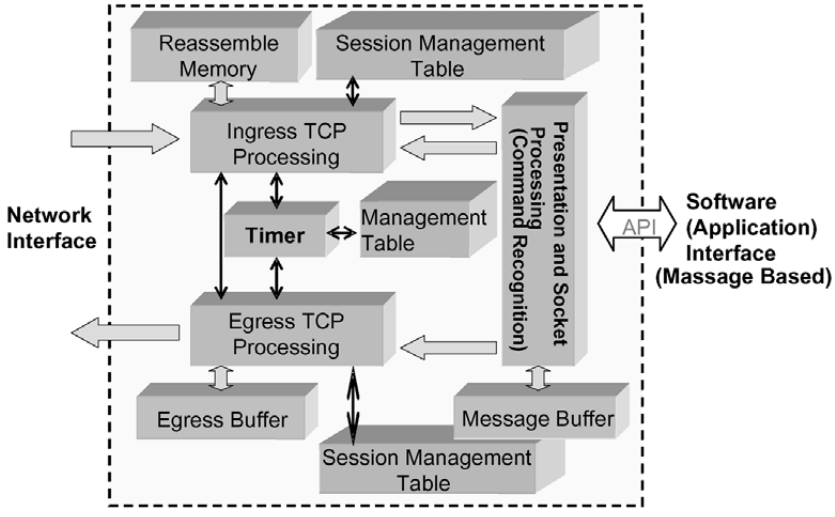

Fig. 7 TCP, Socket and Presentation engine architecture.

Table I TCP, Socket and Presentation engine specification.

Subject	Contents
Processing Performance	Multi-Gigabit Rate
Establishment Performance of Session	160k Connections / sec
Simultaneous Sessions	100k-1M Sessions (Extensional DIMM)
TCP function	Full set of Reno version
Socket and Presentation	SMTP, HTTP, etc 10-100M character / sec

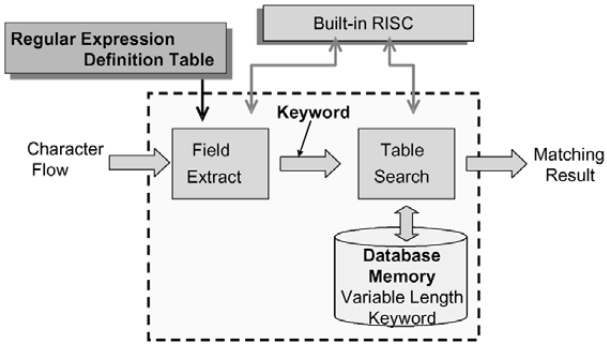

Fig. 8 Contents check engine block diagram.

filter system, this mail filtering system can check 10,000 emails, which have ten keywords in each, in a second. This is 1,000 or more times faster than the existing system.

5. BROADBAND SERVICE GATEWAY SYSTEM PLATFORM

5.1 Realizing New Joint Software and Hardware Architecture

Several hardware engines that have been developed can reduce the load on the operating system software and the application software; this enables the software on a processor to concentrate on higher-level processing. Performance improvement of several orders of magnitude compared to the existing model is also possible when using the whole network front end processing system. The implementation of the new joint software and hardware architecture is shown in **Fig. 9**. The engine board (short title: HACONE) which implements the architecture is shown in **Fig. 10**.

5.2 Stackable & Flexible Architecture

The broadband service gateway platform which mounts the engine boards, the LAN switch and the server board, and unifies the network front end function is shown in **Fig. 11**. The basic architecture of the broadband service gateway is shown in **Fig. 12**.

The network front end function evolves and changes corresponding to the advancement of business applications or services. Moreover, it is also necessary for the function to expand corresponding to the increase in business or the scale of the service. Because the broadband service gateway has started small and will evolve in line with the evolution of the network front end function, Stackable and Flexible architectures (pay as grow architecture) were

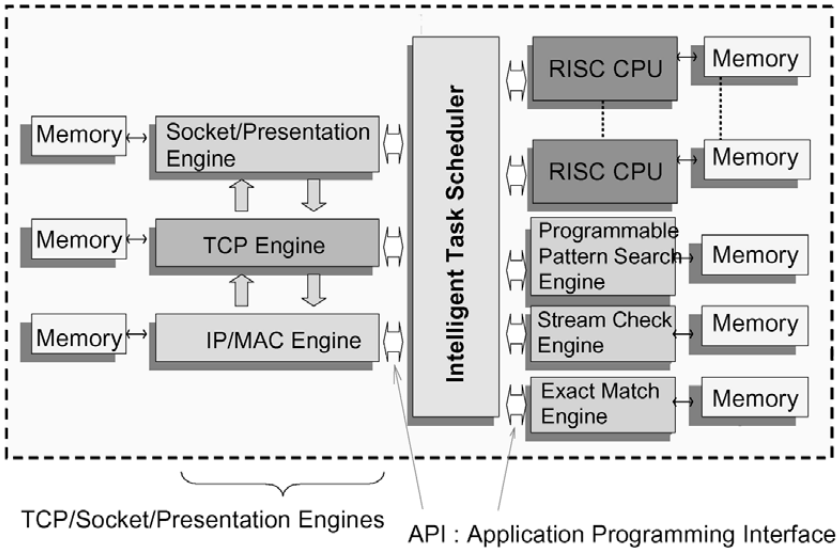

Fig. 9 Software hardware joint architecture.

Fig. 10 Programmable engine board (HACONE).

Fig. 11 Broadband service gateway system platform.

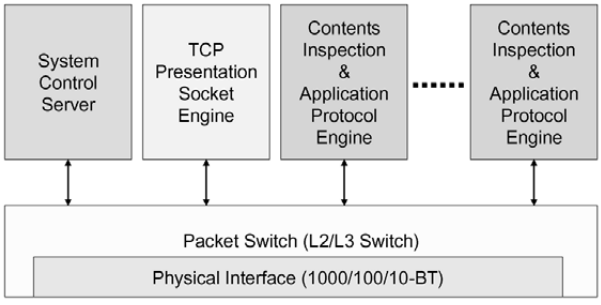

Fig. 12 Broadband service gateway basic architecture.

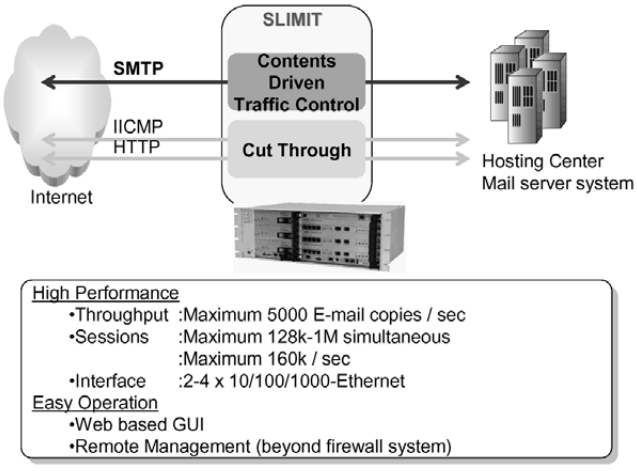

Fig. 13 Specifications and system configuration of SLIMIT.

adopted. Therefore, it is possible at the right time and for optimum cost to enhance the performance and extend the functionality by adding the engine board to the broadband service gateway.

5.3 Contents-Based Mail Traffic Controller as an Application of the Broadband Service Gateway

By using the engine and the system platform which were described above, a contents-based mail traffic controller has been realized and produced commercially (SLIMIT). This system extracts e-mail traffic from the data stream, and identifies a source/destination e-mail address, an e-mail subject name, an e-mail server IP address and the keyword in the e-mail text body. The system controls e-mail traffic by using this extraction and identification method. By using this system, the mail server system can be protected from a lot of unsolicited junk e-mails or server attacks, and is it possible to greatly reduce the load imposed on an e-mail system. Specifications and system configuration of SLIMIT are shown in **Fig. 13**.

6. CONCLUSION

We have succeeded in the development of several engines, and a broadband service gateway platform. A contents-based e-mail traffic controller (SLIMIT) has been developed as an application of this technology. The new joint software and hardware architecture has been realized and it exceeds the performance the existing “general-purpose processor + operating system + application software” architecture. In particular, it enables reduction in the load imposed an information system and protects the information system from application and contents-level cyber-attacks. It achieves this through close cooperation between the network function and the information system function. By implementing the engines of the network front end functions so that they are reliable and have good performance, these functions can be deployed in a network as part of the network system. Also, several applications can be integrated into the network application. When developing new engines in the future, a new environment will be utilized. API (Application Programming Interface) is to be provided to the application developers.

Received April 15, 2004

* * * * * * * * * * * * * * * *

Motoo NISHIHARA received his B.E degree from Tokyo University in 1985. He joined NEC Corporation in the same year and received M.S degree in 1994 from Carnegie Mellon University. He is involved in the research and development of the IT&NW integrated system platform. He is now a Principal Researcher at System Platforms Research Laboratories.

Satoshi KAMIYA received his B.E degree from Tokyo University in 1991 and his M.E degree in 1993. He joined NEC Corporation in 1993. He is involved in researching and developing Integrated IT and Network products. He is now a Principal Researcher at System Platforms Research Laboratories.

Takeo HAYASHI received his B.S degree from Osaka University in 1992 and his M.S degree in 1994. He joined NEC Corporation in 1994. He is involved in the research and development of a Mail filter and security system. He is now an Assistant Manager at System Platforms Research Laboratories.

Hiroshi UENO received his B.E degree from Kyoto University in 1991 and his M.E degree in 1993. He joined NEC Corporation in 1993, and is currently Assistant Manager of NEC Ubiquitous Platform Development Division, Solution Development Laboratories.

Tomoyasu DOMEKI received his B.E degree from Nihon University in 1991. He joined NEC-Miyagi, Ltd. in 1991, and is currently Assistant Manager of NEC Ubiquitous Platform Development Division, Solution Development Laboratories.

Toshiyuki KANOH received his B.E degree from Osaka University in 1981. He joined NEC Corporation in 1981. He is involved in the research and development of the IT&NW integrated system platform. He is now a Chief Manager at System Platforms Research Laboratories.

* * * * * * * * * * * * * * * *