Mr.G.Rambabu, Mr.B.Hanumatha Rao / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.089-095

A Security Architecture For Intranet Based On Security Area Division

Mr.G.Rambabu, M.Tech, Mr.B.Hanumatha Rao, M.Tech,[PhD].
Asst.Professors Dept of C.S.E, Potti Sriramulu College of Engineering and Technology ,Vijayawada; A.P.

Abstract

Aiming at the security requirement of the Intranet that is different from Internet, an security architecture for Intranet is proposed. In physical layer and data link layer, based on network switch the intranet is divided into several parts separated from each other as required. In network layer, making use of the NAT gateway integrated in virtual server the intranet or its part is hidden to ensure its security, and at the same time the other part of the intranet can securely access to the part of hidden resources. Using reliable IP address management and distribution mechanism the IP addresses are kept from being stolen or abused. In application layer, using bi -directional proxy server each part of the Intranet is separated, but the hosts can access each other based on application and user authority. The security switches are used to connect each separate part of the Intranet, based on application as well as user authorization control to carry out network access control. The security architecture focuses on security guarantee of intranet inside the traditional network boundary, and provides foundation framework to Intranet security which can ensure the reliability, usability, confidentiality, integrity, and maneuverability of the Intranet.

Keywords- Network Security; NAT Gateway; Bi-directional Pro; IP Address Management

I. INTRODUCTION

For the Years, a large number of researchers have been dedicated to network security research, and have made tremendous progress. The security architecture of ISO/OSI reference model has been developed by ISO in 1989. In this model, security services, mechanisms, and management are added. Besides, the logical relationship between the OSI network architecture, security service, and security mechanism are given. The five categories security services are also defined. Simultaneously, the eight major security mechanisms of these services and the corresponding Open Systems Interconnection security management are provided [1] [2]. Based on this framework, through continuous improvement, an Internet security architecture which is comparatively mature has been basically formed now. The architecture consists of access control, encryption, data integrity mechanism, authentication mechanisms, system vulnerability detection, security protocols and firewall and intrusion detection technology. However, Internet security architecture focuses on resolving security problems in network border, that is addressed only the security problems of communication between Internet and Intranet [3]. The network communication between the various parts and the running conditions can not be statistical and managed. And there is lack of effective technical means to ensure the security of Intranet. Hence the security of Intranet is a very serious problem. In addition, Intranet security requirements are different from the Internet security requirements. Internet security requirements are mainly concerned about secure in information transmission between different systems. While, what must be considered in Intranet, is safety measures within system, equipment or organization. Priority needs of Intranet security embody in the following aspects: (a) usually, Intranet users can access to, attack and eavesdrop to the other hosts and devices within the network by a simple tool. So isolation with different security levels and rights management are needed in the Intranet. (b) With the development of application demand, it would be probably that the sub-network of Intranet would not be in the same physical space. Then security policy managements for each specific endpoint are needed. (c) In Intranet, resources and data transfers are not in the protection of traditional border security mechanisms. Thereby, it is needed to enhance a set of measurement and control security measures applicable to Intranet.

II.INTRANET SECURITY ARCHITECTURE BASED ON SECURITY AREAS DIVISION

TCP/IP-based applications are increasingly being used within the network, which made the security problem more prominent, but so far, there is not complete Intranet security architecture to prevent these problems. The author with years of practical experience in computer network and a full understanding of security needs analyzes the currently existed intranet security technology and design an Intranet security architecture based on security areas division, as shown in Fig. 1.

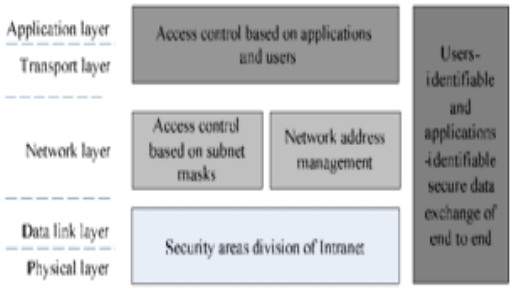

Figure 1.An Intranet security architecture based on security area divison.

(a) In the physical layer and data link layer, according to specific needs, network switches or other network devices are used to divide a large network into a number of mutually isolated subnet (security area), and each subnet can have different security levels.

In the network layer, designs like NAT gateways can be used to screen the subnet that requires security protection, therefore the screened subnet is not visible to the outside, and at the same time, the virtual server can be used to access one or several hosts of the screened subnet.

(c) Secure reliable network address management and distribution mechanism is used to prevent IP address embezzlement or abuse in order to ensure the safe operation of the network.

(d) In the transport layer and application layer, interconnect devices are used to connect isolated subnet, and hosts in different subnet can access each other by using application and user authorization mechanisms.

(e) The secure switches are used to connect the various parts in this isolated Intranet, but hosts in different isolated parts can access each other by using user authorization control or other controls, such as application control, network traffic control, and time control.

Intranet security system architecture based on Fig. 1 is shown in Fig. 2.

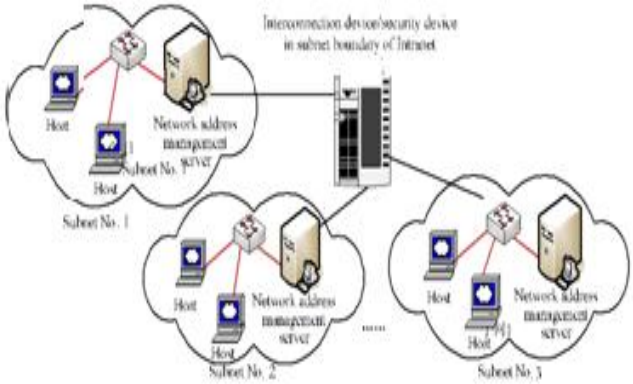

Figure 2. The structure of Intranet security system.

First, switches or other techniques are used to divide the whole Intranet into a number of subnets (security area) with different security level, the security area can be a physical subnet or a logically constitute virtual subnet. In a subnet, network address management server can be used to complete the allocation and management of IP addresses, effectively preventing IP address embezzlement or abuse widely existed in Intranet. Subnet boundary connection device is used to connect among the subnets. Based on different situations, the network layer which is convenient and transparent to users can be chosen to complete interconnection NAT gateways integrated in virtual server, or the application layer with high security can be selected to complete interconnection bidirectional proxy server. Multi-layer security switches can be used to complete security area division in the physical layer, data link layer and network layer. In the transport layer and application layer, user authorization or other applications is adopted to complete end-to-end access among users in the security area.

III.DIVISION OF INTRANET SECURITY AREA

When the Intranet just began to develop, the network size was small, and the application scope was narrow. The understanding on network security and management is light level. Due to all of these and other reasons, the whole Intranet belongs to a local area network normally. That is, all hosts or devices of the network reside in a very same broadcast domain. Supposing that A denotes the set of all the hosts or network devices within Intranet, and B represents the set of all the hosts or network devices of any one broadcast domain in an Intranet. Then:

$$A=B \qquad (1)$$

Intranet with the nature of equation (1) has the advantage of simple structure, easy to use, etc. But shortcomings as follows also exists [4]:

(a) The existence of serious security risks. Any user can attack the other hosts or network devices in the network, or listen in other users' communication data by a simple tool. Virus can easily spread throughout the entire Intranet.

(b) With the expansion of the network, effective traffic decreased significantly. This is mainly because in the Intranet communications among the host or the network devices must use the protocols that broadcast messages periodically, such as ARP. And these broadcast messages share as high as, even more than 50% of the entire network traffic sometimes.

The entire network can be divided into m subnets (security area) according to a certain regulation by using switches. The subnets connect with each other through routers, gateways, proxy servers, etc. Then network security devices can be set up at the boundary devices, so as to ensure the communication security between each subnet, as shown in Fig. 3.

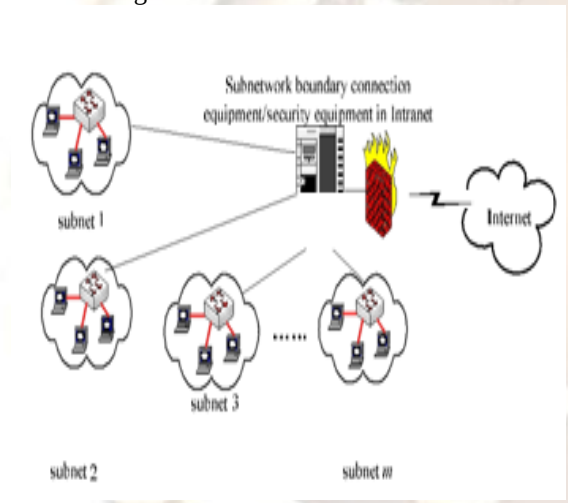

Figure 3. An Intranet divided into subnets

The subnet division shown in Fig. 3 can follow the following principles:

(a) Dividing physical subnets based on physical location. For example, hosts in an office or an office building can be regarded as a subnet.

(b) Dividing the network into VLAN based on the logical relationship. For example, the Intranet can be divided into subnets according to the organization's departments. Then all departments are not necessarily physically adjacent.

It is supposed that, A denotes the set of all the hosts or network devices within Intranet, and B represents the set of all the hosts or network devices of any one broadcast domain in an intranet. Then:

$B_i \subset A$ and $B_1 \cup B_2 \cup \ldots \cup B_m = A$ (2)

Divided into subetworks, the broadcasting is confined to the subnet, making the broadcast traffic within the Intranet greatly reduced. And network security problems are also confined to the subnet. Then the network management becomes convenient.

Supposing that, the Intranet is composed of m hosts, and every host send n broadcast packets per second. Then, for the Intranet without divided into subnets, there are m×n broadcast packets per second in the Intranet. While, if the Intranet is divided into p subnets, and the host number of the largest subnet is q (q<m), the number of broadcast packets per second will be less than q × n.

When the Intranet is divided into some independent and interconnected subnets, each subnet can be managed under the specific circumstances using different security technologies.

IV.NAT GATEWAY WITH VIRTUAL SERVER FUNCTION

A. NAT model

NAT (Network Address Translation) is a standard drafted by IETF (Internet Engineering Task Force) . Network addresses can be mapped from one address space to another address space by NAT technology. NAT technology is used for two purposes: the first purpose is to keep some certain IP addresses for the Intranet reuse, which allows the Intranet only using one or several valid IP addresses to connect the Internet, solving the IP address shortage problem; the second purpose is to hide Intranet IP addresses from the Internet, so that the Internet user can not access the Intranet device directly, which provides protection to Intranet security. NAT model is shown in Fig. 4.

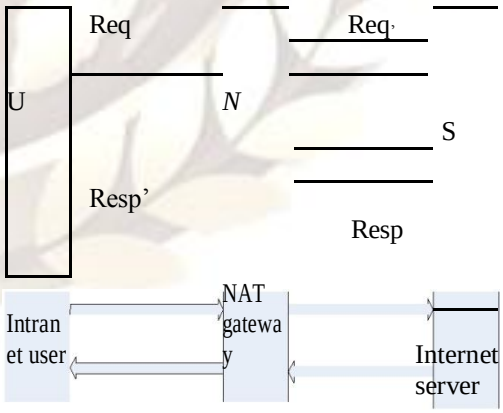

Figure 4. NAT model

Define: NAT function *N*:

$N(Pack,T) \Rightarrow Snd(Md1(Parse(Pack))) \quad T = req$; (3)

$Snd(MdT \Rightarrow 2(Parse(Pack))) \quad resp$;

The structure of *Pack* is *Pack(Header, Data)*. *Header* is the

Pack's head; *Parse(Pack)* is used to parse *Pack* in order to obtain the source IP address and port number; *Md1(Pack)* changes the source IP address and port number obtained by parsing *Pack* into some certain unused public IP address and port number which are visible to the Internet; *Md2(Pack)* changes the destination IP address and port number obtained by parsing *Pack* into user's original request IP address and port number; S*nd (Pack)* sends *Pack* to specified destination, when *T* is a request packet from the intranet to the Internet, it is sent to the Internet destination host, and when *T* is a response packet returned from Internet, it is sent to the Intranet host.

B. Virtual server model

Intranet is invisible to the Internet after using technologies such as NAT, therefore the Internet user can not access to the server in the Intranet. In this situation, a device can be deployed between the Intranets and Internet, which is equipped with at least two network interfaces respectively connected to the Intranet and Internet. The access procedure begin with an Internet host access to the external IP address and a special port of this device, then the device redirects this request to an actual Intranet server based on a set of predefined mapped rules, so far the virtual server technology is explained. Virtual server model is shown in Fig. 5.

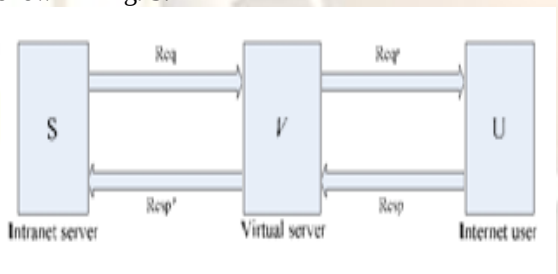

Figure 5. The model of virtual server

Define: Virtual server function V

$$V(Pack,T) \Rightarrow \begin{cases} Snd(Md3(Parse(Pack))) & T \Rightarrow req; \\ Snd(Md4(Parse(Pack))) & T \Rightarrow resp; \end{cases} \quad (4)$$

The structure of *Pack* is *Pack(Header, Data)*. *Header* is the Pack's head; *Parse(Pack)* is used to parse *Pack* in order to obtain the destination IP address and port number; *Md3(Pack)* changes the destination IP address and port number obtained by parsing *Pack* into IP address and port number of the real server in Intranet; *Md4(Pack)* changes the source IP address and port number obtained by parsing *Pack* into IP address and port number opening to the outside on the virtual server. *Snd(Pack)* sends *Pack* to specified destination, when *T* is a request packet from the extranet to the Intranet, it is sent to the Intranet destination host, and when *T* is a response packet returned from Intranet, it is sent to the Internet host.

C. NAT gateway model with virtual server function

A model that combines NAT and virtual server has been proposed, and model is shown in Fig. 6.

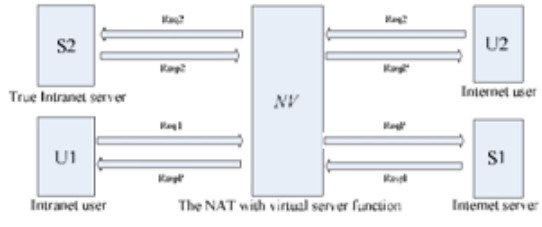

Figure 6. The NAT model with virtual server function

In traditional NAT model, only host in the Intranet can be allowed to send request, and in order to access server located in Internet, the host's IP address and port number have been changed when they reached NAT gateway, so it is a single direction session application that only allows users from the Intranet to send request to the Internet. Usually, there is no problem to connect the Intranet and Intranet with NAT gateway, but if a NAT gateway is used as a border device to connect the subnet in Intranet, there are limits. For example, if security of subnet A has been guaranteed, users in subnet A can access resources in subnet B, at the same time, users in subnet B can access partial open resources in subnet A, and it can be concluded that whether using NAT or virtual server can not complete the such a task.

Define: NAT integrated with virtual server function *NV*

$$NV(Pack,T) \Rightarrow \begin{cases} Snd(Md1(Parse(Pack))) & T \Rightarrow req1; \\ Snd(MdT \Rightarrow 2(Parse(Pack))) & resp1; \\ Snd(Md3(Parse(Pack))) & T \Rightarrow req2; \\ Snd(MdT \Rightarrow 4(Parse(Pack))) & resp2; \end{cases} \quad (5)$$

The structure of Pack is Pack(Header, Data). Header is the Pack's head; Parse(Pack) parses Pack to obtain the source IP address and port number; Md1(Pack) changes the source IP address and port number obtained by parsing Pack into some certain unused public IP address and port number which are visible to the Internet; Md2(Pack) changes the destination IP address and port number

obtained by parsing Pack into user's original request IP address and port number; Md3(Pack) changes the destination IP address and port number obtained by parsing *Pack* into IP address and port number of the true server in Intranet; *Md4(Pack)* changes the source IP address and port number obtained by parsing *Pack* into IP address and port number opening to the outside on the virtual server; *Snd(Pack)* sends *Pack* to specified destination.

V. BIDIRECTIONAL PROXY SERVER

The so-called proxy server refers to an entity that replace client to process connection request to server. When the proxy server requires a connection from the client, it will verify the client's request, and then process the connection request under a specific security program. After delivering the handled request to the true server, the proxy server begins to wait the answer from the sever. When the answer arrived, the proxy server will do a further processing and at last send the handled answer to final client. Proxy server is usually deployed between the Intranet and the Internet, playing an intermediate role when Intranet users applying for the Internet service and acting as a firewall [5]. The advantage of proxy firewall is security. Since each connection between Internet and Intranet needs conversion of the proxy server, and being processed by security application purposely programmed for specific services such as HTTP, FTP, etc., and then the proxy server submits the request and answer itself without leaving any chance of direct session for the hosts both in the Intranet and Internet, thus avoiding the use of data driven type attack in Intranet. But there are limits when the proxy server tries to connect separate subnets in the Intranet. For example, under the premise that security is guaranteed, it is impossible for a proxy server to complete such a task: users in subnet A can access resource in subnet B while some specific users in subnet B can access to resource in subnet A. In order to achieve the above purpose, bidirectional proxy server model is proposed, and the model is shown in Fig. 7.

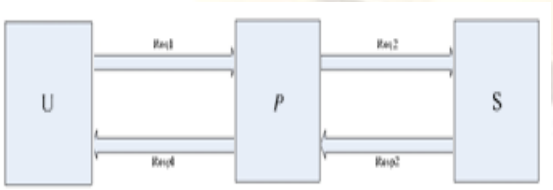

Figure 7.The model of bidirectional proxy server.

The model in Fig. 7 looks similar to the NAT model shown in Fig. 4, but they are different. First, NAT is unidirectional, while the proxy server is bidirectional and symmetric. User (U) and server(S) in proxy server model are either in the Intranet or in the Internet. Second, the two models are in different levels. NAT model is in the network layer and transport layer while bidirectional proxy server model is in the application layer with more security [6].

Define: Proxy server function P

$$P(Msg,T) = \begin{cases} Cont\_Snd(Parse(Msg)) & T = req; \\ Cont\_Snd(Msg) & T = resp; \end{cases} \quad (6)$$

Msg is a application layer packet, and its structure is Msg(Header, Data). The value of Header varies with the application layer protocol; Parse(Msg) is used to parse Msg in order to obtain the URL in it. Based on the destination host and its port number obtained from the URL, Cont_Snd(Msg) is used to establish a connection to the destination host and send the Msg to the specific destination host.

VI. ALLOCATION AND MANAGEMENT OF IP ADDRESS

The rapid development of network makes it more and more extensive used, the number's increasing and the uneven levels of Internet users have also brought many problems to the network security and stability. The IP addresses embezzlement or abuse of Intranet is one of the problems. The main cause of IP addresses embezzlement or abuse is the scarcity of IP address resources and the existence of security vulnerability TCP/IP protocol. Therefore, developing an Intranet IP allocation and management system, and effectively auditing user behavior, what is important to guarantee the network security and service reliability[7][8].

In view of the specific circumstances of IP using in Intranet, a static IP address assignment and management scheme was proposed. The scheme is based on an improved DHCP protocol. It is the model shown in Fig. 8.

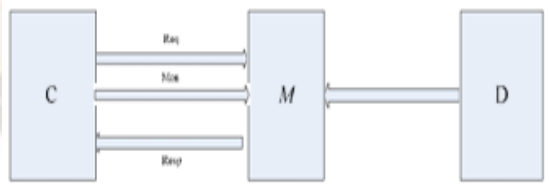

Figure 8. IP address management model.

Definition: IP address management function *M*

$$M(Msg1)=send(Msg2) \quad (7)$$

In equation (7), *Msg1* is a DHCP request that IP address management server *M* receives from the client C, or the ARP broadcast that *M* listen in from the client. When it is the DHCP request, the IP

address correspond to MIC address in *Msg1* will be found from the database D, and then the response message *Msg2* will be formed and sent back to the client C; if *Msg1* is the ARP messages that *M* listen from C, the MIC address and the IP address in and *Msg1* will be checked with the correspondence stored in database D. When there is inconsistent, an ARP response message *Msg2* will be formed according to the correspondence stored in D, and send to C. And then C considers that the IP address has been occupied, and abandons the IP addresses. So as to avoid IP addresses embezzlement or misuse.

VII. END TO END SECURE EXCHANGE OF IENTIFIABLE USER AND APPLICATION

Discussed above is based on the existing network technologies to increase security measures in order to achieve the purpose of network security, but it is the practice of patching. In order to ensure real security, any data exchange between users should been done on the basis of user authentication, and different applications can be identified. Switches play an important role in the Intranet, which are the core of the entire network. Only a switch is integrated security mechanism, can Intranet security problems be solved fundamentally[9].

Common switch is just a simple forwarding device. When a common switch receives a frame from one port, based on the destination MAC address contained in the frame, it will forward the frame from some other port, as the forwarding model shown in Fig. 9.

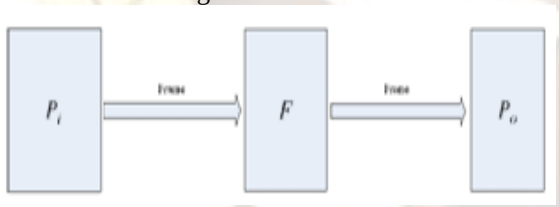

Figure 9. Switch model

Define: switch forwarding function *F*

$$F(Frm) \Rightarrow \begin{cases} Fwd\_Send(Frm) & Mic\_d \in Po; \\ Brd\_Send(Frm) & Mic\_d \notin AnyPo; \end{cases} \quad (8)$$

Frm is frame in data link layer, and its structure is

Frm(Header, Data). *Header* contains the source address *Mic_s* and destination address *Mic_d*. For the switch supporting VLAN, it requires checking whether the source and the destination belong to the same VLAN in the forwarding; for the 3-layer switch, it needs checking whether the souce and destination belong to the same subnet.

For the safety switch, functions such as security authentication, ACL(Access Control List) should be integrated into the switch, and user communication control from end to end should be carried out. ACL is an instruction list which is applied in the safety switch interface, telling the safety switch whether a frame can be received or not. ACL contains authentification. ACL contains certification flag, MAC address, network layer address, transport layer port, For example, A and B are two users who are connected by a security switch, and they have to pass the safety switch certificate before communicating, after adoption of certification, certification flag has been set, which indicates that the two sides can communicate, but not everything can be sent. For example, IP packets can be sent, but not IPX packets (distinguished via the network layer type); TCP messages can be sent, but not some of the ICMP messages with security risk, etc. (distinguished via the transport layer port); video conference can be holden via the network, but not the QQ chat (which can be distinguished by application type); a conversation can be allowed to startup by A, but not B(which can be controlled through the transmission direction in certification) and so on. In addition, it is also necessary for the security switch to have the flow control technology, which limit the traffic within a certain range and avoid the unlimited abuse of the switch bandwidth, like downloading a large number of files, worms' spread and so on. With the technology, the exception flow control is realized, and network congestion is avoided.

VIII. CONCLUSIONS

Aiming at the security requirement of the Intranet which is different from Internet, Intranet security architecture is proposed. In physical layer and data link layer, based on network switch the Intranet is divided into several parts as required. In network layer, making use of the NAT gateway integrated in virtual server the Intranet or its part is hidden to ensure its security, and at the same time the other part of the Intranet can securely access to the part of hidden resources. Using reliable IP address management and allocation mechanism the IP addresses are kept from being stolen or abused. In application layer, using bi-directional proxy server each part of the Intranet is separated, but the hosts can access each other based on application and user authority. The security switches are used to connect each separate part of the Intranet, based on application as well as user authorization to carry out network access control. The security architecture focuses on security guarantee of Intranet inside the traditional network boundary, and provides foundation framework to Intranet security which can ensure the reliability, usability,

confidentiality, integrity, and non-repudiation, controllability of the Intranet. This Intranet security architecture can provide the base framework. According to the architecture, the Intranet security management system has been developed and run in many enterprises. And all the results show that the solution is feasible, and has achieved the purpose of Intranet security.

REFERENCES

[1] D. Y. Hu, Network security. Beijing: Tsinghua university press, 2004.
[2] J. H. P. Eloff and M. M. Eloff, "Information security architecture", Computer Fraud & Security, vol. 2005, No. 11, pp. 10-16, November of 2005.
[3] A. A. Gokhale, "Network security: Typical layout and need for an open systems approach", Journal of the Communications Network, Vol. 2, No. 4, pp. 46-49, October, 2003.
[4] Q. S. He and G. X. Yao, "The analysis of network security requirements and security police research", Computer Engineering, Vol. 26, No. 6, pp. 56-58, June, 2000.
[5] Y. Chen, Z. Z. Li, Z.G. Liao and Z. W. Wang, "Study on placement optimization of web proxies based on genetic algorithm", Journal of Xi'an Jiaotong University, Vol. 39, No. 4, pp. 373-375, April, 2005.
[6] F. X. Gao, Y. Yao, Q. Liu, L. Liang and L. Yao. "Design and implementation of a bi-directional proxy server", Wuhan University Journal of Natural Sciences, Vol. 9, No. 5, pp. 760-764, October, 2004.
[7] S. Q. Yu, and W. Yan, "Limitation and solution of current IP address management for Internet", Journal of Shanghai Normal University, Vol. 29, No. 1, pp. 50-54, January, 2000.
[8] F. X. Gao, H. Yang, X. R. Luo and X. L. Cui, "Intranet-oriented IP address management system", Journal of Harbin Institute of Technology Vol. 38, No. 8A, pp. 1660-1663, August, 2006.
[9] Y. Qian and W. H. Dou, "The design and implementation of SOPC-based security Ethernet chip". China Integrated Circuit, Vol. 11, No. 12, pp. 47-50, December, 2004.